



Purchasing Policies & Procedures

Supplier Code of Conduct, Ethics, and Compliance

Policy #	PUR-GLB-PC-01	Date	23 October 2026	Email	Group purchasing@opex.com
Version	2.0	Contact	Andy Brimelow	Phone	1-856-727-1100

Table of Contents

Purpose 2

Scope 2

Policies and Procedures 2

1. Supplier Expectations 2

2. Labor 3

3. Health and Safety..... 3

4. Environmental 3

5. Information Governance, Cybersecurity, and Intellectual Property 4

6. Other Legal and Regulatory Compliance Requirements 5

7. Other Business, Operational, and Ethical Requirements 6

8. Compliance Monitoring and Verification 8

Related Documents..... 9

Violations..... 9

Approval and Ownership..... 10

Revisions, Revision History, and Related Considerations..... 10

Purpose

This OPEX Supplier Code of Conduct, Ethics, and Compliance (the "Code" or "Policy") establishes the minimum legal, ethical, operational, and business conduct standards that suppliers of hardware, software, materials, components, and any other goods supplied to, or services performed for or on behalf of, OPEX (collectively, "Products") are required to observe when conducting business with, for, or on behalf of OPEX. The Code promotes integrity, responsible corporate conduct, effective risk management, lawful business practices, and business relationships that reflect OPEX's commitment to high ethical standards and compliance with applicable laws and regulations.

Scope

This Policy applies to OPEX Corporation, its affiliates, its/their subsidiaries, and its/their registered branches worldwide (collectively, "OPEX" or the "Company").

Although suppliers are independent entities, their conduct may directly affect OPEX's legal compliance, business operations, customer relationships, and reputation. Accordingly, suppliers are expected to conduct business with, for, or on behalf of OPEX lawfully, ethically, responsibly, and diligently.

Suppliers are expected to comply with this Code, their applicable agreements with OPEX, OPEX's applicable policies, procedures, standards, guidelines, specifications, and other requirements applicable to the supplier or the Products (collectively, the "Applicable Requirements"), as well as all applicable laws, regulations, and legally binding governmental requirements.

Suppliers must take reasonable steps, including, where appropriate, incorporating appropriate requirements into their agreements with their own suppliers, approved subcontractors, agents, and other permitted business partners involved in providing Products to or for OPEX, to promote compliance with the principles and requirements of this Code.

The Code is intended to complement, and should be read together with, the other Applicable Requirements. Suppliers are expected to comply with this Code and the other Applicable Requirements. Where multiple Applicable Requirements address the same subject, suppliers should comply with the more restrictive requirement unless applicable law or the applicable agreement with OPEX expressly provides otherwise. In the event of any conflict between this Code and applicable mandatory law, the applicable mandatory law shall govern. Nothing in this Code is intended to require a supplier to violate applicable law. If a supplier believes that compliance with this Code would require conduct prohibited by applicable law, the supplier shall promptly notify OPEX by contacting Group purchasing@opex.com so that an appropriate course of action may be determined.

The most current version of this Code will be maintained in accordance with OPEX's Policy on Policies and made available on OPEX's website. Suppliers are responsible for ensuring that they are familiar with the current version of this Code.

From time to time, OPEX may approve and make available more detailed or location- or business unit-specific policies, procedures, standards, and processes to address specific information relevant to this Policy. Those additional policies, procedures, standards, and processes, some of which are listed in this Policy under "Related Documents," are extensions of this Policy.

Policies and Procedures

1. Supplier Expectations

Suppliers must conduct their business lawfully, ethically, and in a manner consistent with OPEX's guiding principles and the requirements of this Code. OPEX believes that a shared commitment to these principles provides the foundation for trusted, long-term business relationships.

The guiding principles particularly relevant to suppliers include:

1. Conduct all business in a fair and honest manner.
2. Listen and be responsive to customers' needs.
3. Recognizing the value of the individual.

2. Labor

OPEX expects suppliers to comply fully with all labor laws and regulations and to share OPEX's commitment to recognizing and respecting the value of every individual. Suppliers must, without limitation, adhere to the following:

Anti-Harassment and Anti-Discrimination

Suppliers must maintain a workforce and workplace free of harassment, unlawful discrimination, and retaliation. While OPEX recognizes and respects cultural differences, suppliers must not engage in harassment or discrimination in employment on the basis of race, color, gender, sexual orientation, gender identity, age, religion, national origin, disability status, or any other characteristic protected by applicable local laws and regulations.

Forced and Child Labor

Suppliers must comply with all applicable federal, state, local, and other laws and regulations prohibiting forced labor, slavery, and human trafficking. Suppliers must not use or benefit from forced, bonded, indentured, involuntary, or prison labor, nor engage in human trafficking or similar exploitative labor practices. Furthermore, suppliers must not engage in, support, or knowingly do business with any person or entity that engages in the foregoing activities.

Furthermore, suppliers must not use child labor. The term "child" refers to any person employed under the age of 15 or the minimum age for employment in the country where work is performed, whichever is higher. OPEX supports the use of legitimate workplace apprenticeship programs which comply with all applicable laws and regulations.

Freedom of Association and Collective Bargaining

Suppliers must respect workers' rights to freedom of association and collective bargaining, in accordance with applicable laws and regulations.

Wages, Benefits, and Working Hours

Suppliers must comply with all applicable laws and regulations regarding wages, benefits, and working hours in the locations in which the supplier operates, including, but not limited to, laws and regulations relating to minimum wages, legally mandated benefits, time off, and overtime pay.

3. Health and Safety

Suppliers must comply with all applicable health and safety laws and regulations and provide a healthy and safe working environment that promotes accident prevention and minimizes exposure to health and safety hazards including, without limitation, hazardous conditions and hazardous substances. Suppliers must provide employees with appropriate and well-maintained personal protective equipment (PPE) and training about workplace hazards, as applicable. Health and safety information must be clearly posted in the supplier's facilities in locations readily accessible to workers. Suppliers should encourage workers to report workplace injuries, unsafe conditions, and health and safety concerns without fear of retaliation.

4. Environmental

Suppliers must comply with applicable environmental laws and regulations and conduct their operations in a way that preserves and protects the environment. Suppliers must make information available about

any restricted or regulated substances in Products supplied to OPEX, which includes compliance declarations, material safety data sheets (MSDSs), and other information upon request.

Furthermore, as applicable, suppliers must have processes, procedures, and systems in place to ensure the safe handling, movement, storage, recycling, reuse, and management of waste, air emissions, and wastewater discharges. Any waste, emissions, or wastewater with the potential to adversely impact human or environmental health must be appropriately managed, controlled, and treated prior to release into the environment.

Suppliers must promptly notify OPEX of any actual or suspected environmental incident that could materially affect Products supplied to OPEX or the supplier's ability to perform its obligations.

5. Information Governance, Cybersecurity, and Intellectual Property

Suppliers must protect confidential information, personal data, information systems, and intellectual property and must comply with all applicable laws and regulations relating to privacy, cybersecurity, artificial intelligence, and intellectual property. Without limitation, suppliers must adhere to the following requirements:

Confidentiality

Suppliers must take reasonable precautions to preserve and protect confidential information and must never make or permit any unauthorized disclosure or use of confidential information that it may receive or obtain or to which it may be given access in connection with its relationship with OPEX, whether the information relates to OPEX, any of OPEX's customers, or other suppliers.

Data Protection

Suppliers must comply with all applicable laws and regulations relating to the accessing, collecting, processing, receiving, transmitting, disclosing, storing, and using personal data and other protected or confidential information in connection with any matter involving or relating to OPEX or any Product that the supplier provides to OPEX.

Furthermore, suppliers must maintain appropriate technical and organizational safeguards to protect OPEX information and must notify OPEX promptly of any actual or suspected unauthorized access, disclosure, loss, misuse, or compromise of OPEX information or systems.

Cybersecurity

Suppliers providing Products or services that include software, firmware, digital components, network connectivity, cloud-based functionality, hosted services, or other digital elements must design, develop, manufacture, maintain, and support such Products and services in a manner reasonably intended to protect their cybersecurity, integrity, availability, and resilience throughout the applicable support period. Suppliers must comply with all applicable cybersecurity laws, regulations, contractual requirements, and recognized industry security standards applicable to the Products or services they provide.

Suppliers must implement and maintain appropriate administrative, technical, and organizational safeguards to protect OPEX's information, systems, networks, accounts, and other resources to which they have access. Suppliers must promptly notify OPEX of any actual or suspected cybersecurity vulnerability, incident, unauthorized access, loss, misuse, disclosure, compromise, ransomware attack, malware infection, or other information security issue affecting Products, services, or OPEX information that could reasonably be expected to affect the security, confidentiality, integrity, availability, or lawful use of such Products, services, or information, and must cooperate fully with OPEX in investigating, mitigating, remediating, and recovering from such matters.

Artificial Intelligence

Suppliers using artificial intelligence ("AI") or similar automated technologies in connection with Products supplied to OPEX or in performing services for or on behalf of OPEX must do so responsibly, ethically, and in compliance with all applicable laws, regulations, and OPEX's applicable requirements. Suppliers must not input, upload, or otherwise disclose OPEX's confidential information, proprietary information,

trade secrets, customer information, supplier information, personal data, or any other non-public or protected information into publicly available AI systems or other unauthorized third-party AI systems unless expressly authorized in writing by OPEX.

Intellectual Property

Suppliers must respect and protect proprietary designs, drawings, inventions, trade secrets, patents, copyrights, trademarks, software, know-how, and other intellectual property rights and must never make or permit any unauthorized use, reproduction, disclosure, distribution, modification, or other misuse of any intellectual property or proprietary information that they receive, obtain, access, are licensed to use, or are otherwise permitted to use in connection with their relationship with OPEX, regardless of whether such intellectual property or proprietary information belongs to OPEX, any of OPEX's customers, other suppliers, or any other third party.

6. Other Legal and Regulatory Compliance Requirements

Suppliers must comply with all other applicable laws and regulations including, without limitation, the following:

Anti-Corruption

Suppliers must conduct all business activities in full compliance with the U.S. Foreign Corrupt Practices Act ("FCPA"), the UK Bribery Act 2010, and all other applicable anti-corruption, anti-bribery, anti-money laundering, and related laws and regulations governing the jurisdictions in which the supplier conducts business.

Suppliers must never, directly or indirectly, offer, solicit, promise, authorize, make, request, accept, or provide any bribe, kickback, facilitation payment (except to the extent expressly permitted by applicable law), or any other improper payment or thing of value to obtain or retain business or secure any other improper advantage in connection with any matter involving or relating to OPEX or any Product supplied to OPEX.

Currency Controls and Money Laundering

Suppliers must comply with all applicable currency controls and never directly or indirectly participate in or cooperate with any money laundering scheme in connection with any matter involving or relating to OPEX or any Product that the supplier provides to OPEX.

Trade

Suppliers must comply with all applicable export controls, import laws, customs requirements, economic sanctions, embargoes, anti-boycott laws, and other trade-related laws and regulations governing the transfer, access, export, re-export, import, use, or disclosure of Products, software, technology, technical data, and services.

Suppliers must not provide OPEX with any controlled technology, Product, software, technical data, or service without providing such notices, classifications, licenses, documentation, or other information as may be reasonably necessary to enable OPEX to comply with applicable laws and regulations.

Suppliers must never provide OPEX with any Product that they know or should know has been produced using forced labor, is counterfeit, violates applicable trade restrictions, has an origin other than that represented, or contains any material, component, or part that they know or should know is counterfeit or has an origin other than that represented.

Suppliers must not participate in, support, or cooperate with any boycott that is prohibited by applicable laws or regulations.

Competition and Antitrust

Suppliers must compete fairly and comply with all applicable competition, antitrust, and unfair competition laws and regulations. Suppliers must not enter into any agreement, arrangement, or understanding with competitors relating to prices, bids, customers, markets, territories, production, or any other matter

prohibited by applicable law. Suppliers must not exchange competitively sensitive information except as permitted by applicable law.

7. Other Business, Operational, and Ethical Requirements

Suppliers must otherwise conduct their business interactions and activities with integrity, honesty, and professionalism, including, without limitation, in accordance with the following additional business, operational, and ethical requirements:

Access to OPEX/Customer Premises and Other Resources

If the supplier's personnel will be visiting or working at OPEX's or an OPEX customer's facility, such personnel are to report to the front desk at the facility and to sign-in upon entering the facility. Supplier personnel accessing an OPEX or OPEX customer facility that does not maintain a front desk receptionist must be escorted by a designated OPEX or OPEX customer employee or by the supervisor in charge. Supplier personnel must not, for security and safety reasons, roam buildings unaccompanied.

External doors and locked internal doors within OPEX and OPEX customer facilities are to remain closed and locked. Suppliers must never prop open doors or leave them unlocked.

If supplier personnel require building keys or other devices (e.g., card keys) to access OPEX facilities, an account on OPEX's email system, and/or other access to any other OPEX system, network, or application, the supplier must sign all applicable OPEX policies and other documents required for such access and use.

Suppliers and their employees must not use their access to OPEX's facilities, systems, networks, applications, or other OPEX resources to obtain information, materials, or other accommodations other than as expressly authorized by OPEX.

OPEX may issue building keys, other access devices, and identification cards to supplier personnel who have a recurring business need to gain entry to OPEX's facilities without an escort and/or the need to identify themselves to other parties as performing work for OPEX.

Any building key or access device issued to a supplier must: (i) be safeguarded by the supplier; (ii) only be used by the authorized recipient; (iii) not be transferred by the supplier without OPEX's express consent to anyone other than the holder authorized by OPEX; (iv) not be duplicated by the supplier without OPEX's express consent; and (v) be returned to OPEX immediately when the employment of its authorized holder is terminated, its authorized holder no longer requires the building key or access device, or OPEX requests return.

Supplier personnel are not permitted to bypass OPEX's official corporate processes for issuing building keys, access devices (e.g., card keys), passwords, or similar credentials, for example, by borrowing such items informally from OPEX personnel or other OPEX suppliers.

If OPEX issues identification cards to the supplier, the supplier's personnel must wear such identification whenever they are at OPEX's premises or an OPEX customer's premises. The identification card must be returned to OPEX immediately: (i) when the employment of its authorized holder is terminated; (ii) when its authorized holder no longer requires such identification; or (iii) at the request of OPEX. Such identification must be used strictly in accordance with all requirements and limitations on its use.

Suppliers who are authorized to access OPEX's systems, networks, applications, information, or other resources may do so only as expressly permitted by OPEX and in accordance with the requirements of OPEX. The supplier must protect OPEX-issued access credentials such as passwords, user IDs, and PINs at all times. Furthermore, suppliers must remove access to OPEX systems, networks, applications, information, and other resources immediately for any supplier personnel, including approved subcontractor personnel, who have been terminated or reassigned.

Monitoring by OPEX applies to OPEX facilities and various other OPEX resources such as company-provided communications devices, systems, and networks (including without limitation corporate email, encrypted and unencrypted Internet access, and any application, such as web-based email accessed

from OPEX-provided devices, networks, systems, and accounts), to the fullest extent permitted by applicable laws and regulations.

OPEX will not be responsible for loss, damage, theft, or disappearance of any personal property or vehicles located on OPEX's premises belonging to suppliers, the suppliers' personnel, or the supplier's approved subcontractors' personnel. If a supplier becomes aware of any personal injury, property damage, loss, or breach occurring on OPEX's premises or involving an OPEX resource such as an OPEX system, network, account, or information, the supplier must notify OPEX promptly and provide adequate details to enable OPEX to investigate the cause.

Business Continuity and Operational Resilience

Suppliers whose Products or services are material to OPEX's business operations must maintain reasonable business continuity, disaster recovery, cybersecurity incident response, and crisis management plans appropriate to the nature, size, and risks of their business. Suppliers must periodically review and update such plans and, to the extent reasonably practicable, test their effectiveness.

Suppliers must promptly notify OPEX of any event that materially disrupts, or is reasonably likely to materially disrupt, the supplier's ability to provide Products or services to OPEX and must cooperate with OPEX in minimizing the impact of such disruption.

Upon OPEX's reasonable request, suppliers must provide information reasonably necessary to demonstrate compliance with this requirement.

Conduct While OPEX/Customer On-Premises or Using Other Resources

While on OPEX's premises, the premises of OPEX's customers, or using other OPEX resources, supplier personnel must conduct themselves in a manner that is respectful of others, complies with this Code, and otherwise complies with all applicable laws and regulations and other rules. Supplier personnel who engage in behavior that infringes on the rights of others, poses a danger or risk to themselves, others, property, or other resources, or violates this Code or applicable laws, regulations, or other rules, may be asked to leave the premises or cease using the resource as applicable and may be subject to other remedial action by OPEX or others.

Unacceptable conduct on OPEX's and its customers' premises includes without limitation:

- Engaging in activities that do not serve OPEX's or OPEX's customers' business interests;
- Maintaining an unacceptable standard of personal hygiene;
- Being inappropriately attired or, as applicable, failing to wear required personal protective equipment (PPE);
- Failing to follow OPEX's or its customer's other health and safety requirements (e.g., any pandemic/epidemic safeguards at OPEX's or OPEX's customers' premises);
- Engaging in the unauthorized destruction of property or the theft of property;
- Using or being under the influence of alcohol or illegal drugs;
- Engaging in lewd, indecent, disruptive, or boisterous behavior;
- Threatening, harassing (sexually or otherwise), or intimidating others; and/or
- Posing a threat to persons or property.

Additionally, OPEX is committed to a 'smoke-free' working environment. Therefore, smoking on OPEX's premises or at the premises of OPEX's customers is strictly prohibited, except in areas (if any) specifically designated as 'Smoking Areas.' Under no circumstances may supplier personnel smoke in an OPEX or customer work area or inside an OPEX vehicle. The smoking restrictions above apply to the use of all tobacco products, regular cigarettes, as well as "e-cigarettes."

Conflicts of Interest

Suppliers must not directly or indirectly offer, make, or provide any personal favor, loan, gift, or another benefit to an OPEX director, officer, or employee or a spouse or other close family member of an OPEX director, officer, or employee other than a casual favor or reasonable entertainment or non-money gift of nominal value that could not reasonably be expected to influence decisions related to the supplier or the Products and otherwise not give rise to a conflict of interest with OPEX.

Furthermore, suppliers must not have any direct or indirect ownership, employment, consulting, financial, or other arrangement or relationship with an OPEX director, officer or employee or a spouse or other close family member of an OPEX director, officer, or employee that could potentially influence decisions related to the supplier or its Products or otherwise give rise to a conflict of interest with OPEX. (The only exception would be an arrangement or relationship that has been fully disclosed to and approved in writing by OPEX's Vice President-Corporate & Legal Affairs, whose contact information is set forth at the end of this Code).

Press

Suppliers may only speak to the press on behalf of OPEX or its customers if expressly authorized in writing to do so by either an OPEX communications representative or the customer's communications representative.

Publicity

Suppliers will not issue press releases or other publicity related to its contracts or relationship with OPEX without the prior written consent of OPEX. This includes without limitation the use of OPEX's name or logo on a supplier's site without the prior written consent of OPEX.

Travel and Other Reimbursable Expenses

To the extent that a supplier is contractually entitled to reimbursement from OPEX for travel or other expenses, the supplier must comply with OPEX's applicable travel and expense policies and guidelines, copies of which will be provided to the supplier upon request.

8. Compliance Monitoring and Verification

OPEX expects suppliers to maintain effective compliance programs and cooperate with reasonable compliance monitoring and verification activities:

- Suppliers shall establish and maintain policies, procedures, processes, and internal controls reasonably designed to ensure compliance with this Code.
- Suppliers shall take reasonable steps to ensure that their own suppliers, approved subcontractors, agents, and other permitted representatives involved in providing Products to or for OPEX comply with the applicable requirements of this Code.
- Suppliers shall promptly report any known or suspected violation of this Code that is relevant to the supplier's business relationship with OPEX and permit their personnel to report actual or suspected violations without fear of retaliation, reprisal, or other adverse action.
- Suppliers who are uncertain regarding the meaning, application, or requirements of this Code are encouraged to seek clarification from their primary OPEX business contact. If that is not appropriate or practical, the supplier should contact OPEX at Group purchasing@opex.com.
- OPEX may require suppliers to confirm and certify their acceptance of and compliance with this Code, complete compliance questionnaires or other reasonable requests for information, permit OPEX or its designated representatives to audit or otherwise verify compliance with this Code (subject to applicable contractual confidentiality obligations), and reasonably cooperate with any audit or compliance verification activities.

Related Documents

- OPEX's Supply Chain Regulatory Requirements, LEG-GLB-SPECS-1.0 (Version 1.0, effective 23 October 2026)

Violations

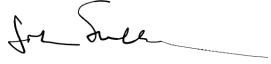
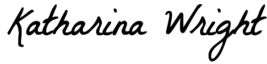
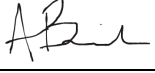
Each supplier to whom a copy of this Code has been provided or its contents communicated is expected to have read and understood this Code. Compliance with this Code is a condition of doing business with OPEX.

Any violation of this Code may result in corrective action and other appropriate remedies, up to and including suspension or termination of the supplier's business relationship with OPEX, termination of any applicable purchase order or agreement, or the exercise of any other rights and remedies available to OPEX under applicable law or contract.

Violations of this Code should be reported to OPEX at Group purchasing@opex.com.

This Code does not create any contractual rights in favor of any supplier or other third party.

Approval and Ownership

Owner	Title	Date (DD-MM-YYYY)	Signature
Andy Brimelow	Director of Purchasing	12 / 10 / 2026	
John Sullivan	International Counsel	12 / 10 / 2026	
Katharina Wright	Manager of Compliance & Regulation	14 / 10 / 2026	
Approved By	Title	Date (DD-MM-YYYY)	Signature
Andy Brimelow	Director of Purchasing	12 / 10 / 2026	

Revisions, Revision History, and Related Considerations

Version	Description	Revision Date	Review Date	Reviewer/Approver Name
1.0	Initial Release (as Policy #S001)	23 January 2022	TBD	John Sullivan, International Counsel; James M. Liebler, Vice President, Corp. & Legal Affairs (retired)
2.0	Major Revision <i>Renumbering of policy; reformatting of policy to align with OPEX's policy on policies; review and updates to key content</i>	23 October 2026	TBD	Andy Brimelow, Director of Purchasing; J. Sullivan, International Counsel; Katharina Wright, Manager of Compliance & Regulation

Title	Supplier Code -- For Your Dropbox Sign Signatures
File name	OPEX_Supplier_Cod..._23_Oct_2026.docx
Document ID	0f680f9c7fb5a4b3fa703f1bdbff027bca16bf02
Audit trail date format	DD / MM / YYYY
Status	● Signed

Document History



12 / 10 / 2026
08:02:18 UTC

Sent for signature to John Sullivan (jsullivan@opex.com), Andy Brimelow (abrimelow@opex.com) and Katharina Wright (kwright@opex.com) from jsullivan@opex.com
IP: 87.140.46.2



12 / 10 / 2026
08:02:20 UTC

Viewed by John Sullivan (jsullivan@opex.com)
IP: 87.140.46.2



12 / 10 / 2026
08:06:58 UTC

A new document has been created based off of an existing document with ID 0f680f9c7fb5a4b3fa703f1bdbff027bca16bf02
IP: 87.140.46.2



12 / 10 / 2026
08:06:58 UTC

Edited by John Sullivan (jsullivan@opex.com)
IP: 87.140.46.2



12 / 10 / 2026
08:06:58 UTC

Signature request resent by John Sullivan (jsullivan@opex.com)
IP: 87.140.46.2

Title	Supplier Code -- For Your Dropbox Sign Signatures
File name	OPEX_Supplier_Cod..._23_Oct_2026.docx
Document ID	0f680f9c7fb5a4b3fa703f1bdbff027bca16bf02
Audit trail date format	DD / MM / YYYY
Status	● Signed

Document History



12 / 10 / 2026
08:07:13 UTC

Viewed by John Sullivan (jsullivan@opex.com)
IP: 87.140.46.2



12 / 10 / 2026
08:07:22 UTC

Signed by John Sullivan (jsullivan@opex.com)
IP: 87.140.46.2



12 / 10 / 2026
08:08:52 UTC

Viewed by Katharina Wright (kwright@opex.com)
IP: 45.41.142.94



12 / 10 / 2026
13:29:29 UTC

Viewed by Andy Brimelow (abrimelow@opex.com)
IP: 104.223.71.123



12 / 10 / 2026
13:30:25 UTC

Signed by Andy Brimelow (abrimelow@opex.com)
IP: 50.232.139.104



14 / 10 / 2026
09:10:48 UTC

Signed by Katharina Wright (kwright@opex.com)
IP: 91.24.130.245



14 / 10 / 2026
09:10:48 UTC

The document has been completed.