
	<b>Title: Global Anti-Corruption Policy</b>	<b>Procedures</b>	<b>OWL-LG-PO-003</b>
	<b>Area: Legal Department</b>	<b>Initial Issue Date:</b>	<b>09/01/2022</b>
	<b>Approval: Counsel</b>	<b>Version:</b>	<b>01</b>
	<b>Page 1 of 11</b>	<b>Revision Date:</b>	<b>May 30, 2023</b>

## TABLE OF CONTENTS

<b>1.0</b>	<b>PURPOSE</b> .....	<b>2</b>
<b>2.0</b>	<b>SCOPE</b> .....	<b>2</b>
<b>3.0</b>	<b>RESPONSIBILITY</b> .....	<b>2</b>
<b>4.0</b>	<b>DEFINITIONS</b> .....	<b>4</b>
4.1	Anti-Corruption .....	4
4.2	FCPA-Foreign Corruption Practices Act .....	4
4.3	Kickback.....	4
4.4	Extortion .....	5
4.5	Bribery.....	5
4.6	Anything of Value .....	5
4.7	Government.....	5
4.8	Government Official.....	5
4.9	Non-U.S. Person .....	5
<b>5.0</b>	<b>POLICY</b> .....	<b>6</b>
5.1	Bribery Prohibited .....	6
5.2	Business Courtesies.....	6
5.3	Charitable Donations .....	7
5.4	Political Contributions .....	7
5.5	Facilitation Payments .....	8
5.6	Understand Local Laws .....	8
5.7	Due Diligence .....	8
5.8	Mandatory Screening .....	8
5.9	Recordkeeping .....	9
5.10	Anti-Corruption Reporting.....	9
5.11	Foreign Corrupt Practices Act (FCPA).....	9
5.12	Anit-Kickback Act of 1986.....	10
5.13	Conflicts of Law .....	10
5.14	Audits and Reviews.....	11
<b>6.0</b>	<b>COMPLIANCE</b> .....	<b>11</b>
6.1	Code of Conduct: The Owl Cyber Commitment .....	11
6.2	Foreign Corruption Practices Act FCPA of 1977 .....	11
6.3	United Kingdom Bribery Act of 2010.....	11
6.4	Anti-Kickback Act of 1986.....	11
6.5	Federal Acquisition Regulations .....	11
<b>7.0</b>	<b>REFERENCES AND/OR FORMS</b> .....	<b>11</b>
<b>8.0</b>	<b>RECORD RETENTION AND DISPOSITION</b> .....	<b>11</b>
<b>9.0</b>	<b>REVISION HISTORY</b> .....	<b>11</b>

	<b>Title: Global Anti-Corruption Policy</b>	<b>Procedures</b>	<b>OWL-LG-PO-003</b>
	<b>Area: Legal Department</b>	<b>Initial Issue Date:</b>	<b>09/01/2022</b>
	<b>Approval: Counsel</b>	<b>Version:</b>	<b>01</b>
	<b>Page 2 of 11</b>	<b>Revision Date:</b>	<b>May 30, 2023</b>

## 1.0 **PURPOSE**

Owl Cyber Defense Solutions, LLC (“Owl Cyber Defense” or “Company”) is committed to the highest standards of business conduct. Owl Cyber Defense’s Global Anti-Corruption Policy (“Policy”) is designed to ensure that Owl Cyber Defense officers, employees, consultants, agents, contract labor, resellers, suppliers, and representatives (collectively referred to as “Representatives”) understand and comply with applicable anti-corruption laws and regulations, whether these laws are from the United States or the country of operations. This Policy supplements the *Code of Conduct: The Owl Commitment* (or the *Supplier/Reseller Code of Conduct*, as applicable) (the “Code”). Both this Policy and the Code must be read together; where there is a perceived conflict, the most restrictive language shall apply.

The U.S. Foreign Corrupt Practices Act (“FCPA”), the United Kingdom Bribery Act and the Anti-Kickback Act of 1986 (41 U.S.C. 51-58) are among the most stringent anti-corruption laws in the world and cover Owl Cyber Defense’s international activities in many cases. Every other country where Owl Cyber Defense conducts business has some form of anti-corruption law in place. These laws generally prohibit payment or offers of even small amounts to government officials. Penalties for violating anti-corruption laws can be severe. Corporate violations can result in multimillion-dollar fines, and individuals can be personally responsible for significant fines or imprisonment for violating anti-corruption laws. In addition, Owl Cyber Defense would deem non-compliance with applicable anti-corruption laws to be a breach of this Policy and our Code resulting in employee discipline, up to and including termination.

## 2.0 **SCOPE**

This Policy applies to all Owl Cyber Defense officers, employees, consultants, agents, contract labor, resellers, suppliers, and representatives (collectively referred to as “Representatives”) at any location on or off Owl Cyber Defense properties at all worksites and locations, both foreign and domestic.


If you have information about a possible violation of this Policy, contact the Legal Department or the ethics email at [ethics@owlcyberdefense.com](mailto:ethics@owlcyberdefense.com). Information provided to the ethics email address is confidential.

## 3.0 **RESPONSIBILITY**

It is the overall responsibility of Owl Cyber Defense’s Legal Department to implement and maintain this Policy. Additional assignments are as follows:

### **Legal Department**

- Annual Policy Distribution: Arrange for distribution of an electronic copy of the Policy to every Owl Cyber Defense employee at least one time per year. For the


	<b>Title: Global Anti-Corruption Policy</b>	<b>Procedures</b>	<b>OWL-LG-PO-003</b>
	<b>Area: Legal Department</b>	<b>Initial Issue Date:</b>	<b>09/01/2022</b>
	<b>Approval: Counsel</b>	<b>Version:</b>	<b>01</b>
	<b>Page 3 of 11</b>	<b>Revision Date:</b>	<b>May 30, 2023</b>

purposes of this Policy, distribution may consist of posting on the Owl Cyber Defense Intranet, employee boards, or e-mail distribution.

- **Annual Training:** The Legal Department is responsible for making sure that that all employees, consultants and contract labor complete annual training. The training component can be an electronic training module or in-person training for purposes of this Policy.
- **Charitable Donations:** Perform due diligence on requests for charitable donations outside the United States that have been otherwise approved by Owl Cyber Defense senior leadership. Determine the appropriate level of due diligence for each request based on the source of the request and the risk environment. The charitable contribution shall not be made if there is information demonstrating a compliance risk.
- **Compliance Support:** Address anti-corruption questions and concerns from Representatives in a timely and thorough manner. Owl Cyber Defense will provide the Legal Department with the necessary resources to support compliance with this Policy.
- **Third-Party Non-U.S. Person Due Diligence:** The Legal Department will work with the Owl Cyber Defense Representative requesting to enter into an agreement or contract with a Non-U.S. Person third-party, to receive all information necessary from the requestor to perform a third-party due diligence review. Mandatory Screening shall be performed before the party can be brought under any type of agreement. The appropriate individuals in the Legal Department shall work with the requestor to submit the compliance review.
- **Enhanced Screening:** If there is a heightened level of risk based on the factual circumstances or any “red flags” from the initial due diligence screening, the Legal Department must ensure that an enhanced diligence assessment is conducted by a third-party service provider. Prior to performing any Enhanced Screening, the Chief Operating Officer (“COO”) must approve of the enhanced screening. If the COO does not approve of the Enhanced Screening, then Owl Cyber Defense will not enter into any arrangements with that Non-U.S. Person.
- **Automated Re-Screening:** Non-U.S. Persons who Owl Cyber Defense does business with should be re-screened at least once per year.
- **Recordkeeping:** Maintain a separate permanent file containing all written records related to anti-corruption compliance. A record of all non-Enhanced Screening due diligence reports is also kept with the sales file for the particular order or company.

### **Human Resources**

- **New Hires:** Distribute a copy of the Policy to every newly-hired employee prior to the new employee performing any job functions.

	<b>Title: Global Anti-Corruption Policy</b>	<b>Procedures</b>	<b>OWL-LG-PO-003</b>
	<b>Area: Legal Department</b>	<b>Initial Issue Date:</b>	<b>09/01/2022</b>
	<b>Approval: Counsel</b>	<b>Version:</b>	<b>01</b>
	<b>Page 4 of 11</b>	<b>Revision Date:</b>	<b>May 30, 2023</b>

- Recordkeeping: Maintain all anti-corruption compliance records for newly-hired employees in official company files.
- Every employee, consultant and contract labor must complete the Owl Cyber Defense Anti-Corruption Training component each calendar year. The Human Resources Department shall maintain a written record demonstrating training has been completed by each Owl Cyber Defense employee, consultant and contract labor.

**Legal/Contracts/Procurement**

- Mandatory Anti-Corruption Contract Term: Ensure that all written agreements issued by Owl Cyber Defense include a standard provision requiring annual certification of anti-corruption compliance before the agreement is executed by Owl Cyber Defense.
- Recordkeeping: Maintain all anti-corruption compliance records in official company files.

**4.0 DEFINITIONS**

The following terms defined herein are provided for context and clarity and should be applied when associated with this Policy to help in understanding the requirements.

**4.1. Anti-Corruption**

Anti-corruption laws generally prohibit offering or accepting anything of value to secure an improper advantage to obtain or retain business. In other words, anti-corruption laws prohibit bribery. While it may be common sense that bribery is illegal, defining what is and is not a bribe may be more complicated. For instance, a gift or payment in one country might be considered a legitimate and customary business practice, while in another country that same conduct would be an illegal bribe.

**4.2. FCPA – Foreign Corruption Practices Act**

The Foreign Corrupt Practices Act of 1977, as amended, 15 U.S.C. §§ 78dd-1, et seq. ("FCPA"), was enacted for the purpose of making it unlawful for certain classes of persons and entities to make payments to foreign government officials to assist in obtaining or retaining business. Specifically, the anti-bribery provisions of the FCPA prohibit the willful use of the mails or any means of instrumentality of interstate commerce corruptly in furtherance of any offer, payment, promise to pay, or authorization of the payment of money or anything of value to any person, while knowing that all or a portion of such money or thing of value will be offered, given or promised, directly or indirectly, to a foreign official to influence the foreign official in his or her official capacity, induce the foreign official to do or omit to do an act in violation of his or her lawful duty, or to secure any improper advantage in order to assist in obtaining or retaining business for or with, or directing business to, any person.

**4.3. Kickback**

“ Kickback” means any money, fee, commission, credit, gift, gratuity, thing of value, or compensation of any kind which is provided, directly or indirectly, to any prime contractor,



<b>Title: Global Anti-Corruption Policy</b>	<b>Procedures</b>	<b>OWL-LG-PO-003</b>
<b>Area: Legal Department</b>	<b>Initial Issue Date:</b>	<b>09/01/2022</b>
<b>Approval: Counsel</b>	<b>Version:</b>	<b>01</b>
<b>Page 5 of 11</b>	<b>Revision Date:</b>	<b>May 30, 2023</b>

prime contractor employee, subcontractor, or subcontractor employee for the purpose of improperly obtaining or rewarding favorable treatment in connection with a prime contractor in connection with a subcontract relating to a prime contract.

**4.4. Extortion**

The crime of obtaining money or some other thing of value by the abuse of one's office of authority

**4.5. Bribery**

Money or favor given or promised in order to influence the judgement or conduct of a person in a position of trust.

**4.6. Anything of Value**

Money or anything that has value to the recipient, such as gifts, favors, travel expenses, charitable donations, or political contributions.

**4.7. Government**

Any agency, instrumentality, department, ministry, or other body of any U.S or non-U.S. national, state, or local government, or any public international organization, including any governmental committee or commission and regulatory agency, and any U.S or non-U.S. government-owned or government-controlled business, corporation, company, or society, or any U.S or non-U.S. political party.


**4.8. Government Official(s)**

- Official (elected, appointed, career, or member), employee, or other Third-Party of a Government;
- Official, employee, or other Third-Party of a public international organization (e.g., Red Cross, United Nations, World Bank, European Union, World Trade Organization, World Customs Organization, North Atlantic Treaty Organization);
- Individual acting for or on behalf of a Government, even though he or she may not be an employee of such Government (such as an uncompensated honorary official or a member of a royal family);
- Official of a political party or candidate for political office inside or outside the U.S.; or,
- Individual who is considered a Government Official under applicable local law.

Note: An employee of a government-owned or government-controlled business is considered a "Government Official" and is subject to the same restrictions under this Policy as an official, employee or Third-Party of a Government. If you have any question as to whether a person (e.g., potential or current customer or vendor) is considered a "Government Official" under this Policy, please contact the Legal Department.

**4.9. Non-U.S. Person**

Any person who is not a U.S. Person. A U.S. Person is defined as a U.S. Citizen, a permanent resident alien (green card holder) or a "Protected Individual" as that term is defined 8 U.S.C. 1324b(a)(3) and any corporation, partnership, or other organization organized under the laws of the United States.

	<b>Title: Global Anti-Corruption Policy</b>	<b>Procedures</b>	<b>OWL-LG-PO-003</b>
	<b>Area: Legal Department</b>	<b>Initial Issue Date:</b>	<b>09/01/2022</b>
	<b>Approval: Counsel</b>	<b>Version:</b>	<b>01</b>
	<b>Page 6 of 11</b>	<b>Revision Date:</b>	<b>May 30, 2023</b>

## 5.0 **POLICY**

Anti-corruption compliance is a priority for a number of reasons beyond these potential penalties. First, any form of corrupt business conduct is in direct conflict with the business ethics of Owl Cyber Defense. Second, corruption can compromise national and international security interests because illegal or off-book payments can support drug trafficking, the proliferation of weapons, funding of criminal or terrorist organizations, and other conduct that impairs our national and international security interests.

Complying with anti-corruption laws in multiple jurisdictions can be complicated but following one simple rule will help ensure compliance in every situation: If you suspect or identify a potential corruption risk, immediately notify the Owl Cyber Defense Legal Department. Owl Cyber Defense will provide the appropriate professional resources to support you and help ensure full legal compliance.


Owl Cyber Defense Representatives must adhere to the following mandatory compliance directives. Non-compliance with these directives would be considered a breach of this Policy and may result in employee discipline or termination of the relationship with Owl Cyber Defense (non-employees).

### 5.1 **Bribery Prohibited**

Owl Cyber Defense prohibits offering, giving, or accepting anything of value with the intent to obtain or retain business for an improper advantage. This applies to U.S. and foreign government officials, as well as commercial parties. No “official” or “commercial” bribery is permitted. Owl Cyber Defense Representatives shall not offer, give or receive anything of value if that conduct could be perceived as making or taking a bribe. Indirect misconduct, such as offering or accepting a bribe through a third-party intermediary or “turning a blind eye” to illegal or improper conduct, is a violation of anti-corruption laws as well as this Policy. Requests or demands for a bribe or other payment might take the form of a personal threat to the health or safety of a person. If you have any questions or concerns about whether offering, giving, or receiving anything of value might be a violation of this Policy, you must consult the Legal Department before proceeding. If a demand for a bribe or payment request is made, you must notify the Owl Cyber Defense Legal Department as soon as possible. If you are not able to notify the Owl Cyber Defense Legal Department in advance of making a payment, you must notify them as soon as possible after making the payment and document any transactions in accordance with the provisions of this Policy.

### 5.2 **Business Courtesies**

A business courtesy is a gift (anything of value) provided to a business counterparty, to include among other things meals, refreshments, entertainment, and admission to sporting events. In certain situations, the exchange of limited, non-cash business courtesies may be appropriate.

	<b>Title: Global Anti-Corruption Policy</b>	<b>Procedures</b>	<b>OWL-LG-PO-003</b>
	<b>Area: Legal Department</b>	<b>Initial Issue Date:</b>	<b>09/01/2022</b>
	<b>Approval: Counsel</b>	<b>Version:</b>	<b>01</b>
	<b>Page 7 of 11</b>	<b>Revision Date:</b>	<b>May 30, 2023</b>

The Company does not seek to improperly influence the decisions of its business counterparties or government officials by offering business courtesies, and the Company requires that the decisions of directors, officers, and employees at the Company not be affected by having received a business courtesy.

Owl Cyber Defense prohibits the solicitation, directly or indirectly, for its benefit or for the benefit of another person, of any gift, favor, or other gratuity or thing of value from a person or organization with which Owl Cyber Defense does business or that seeks to do business with Owl Cyber Defense. Soliciting a gift, favor, or other gratuity or thing of value is strictly prohibited regardless of the nature or value of the item or service.

The Company and its employees may not accept business courtesies that constitute, or could be reasonably perceived as constituting, unfair business inducements or that could violate law, regulation, or policies of Owl Cyber Defense or its customers or could reflect negatively on the Company's reputation.

There are strict laws and regulations on offering gifts or anything else of value apply to activities involving US Government employees, and employees of U.S. Government prime contractors and subcontractors – consult *Owl Cyber Defense's Code of Conduct: The Owl Cyber Defense Commitment* (or the *Supplier/Reseller Code of Conduct*, as applicable).


All Owl Cyber Defense employees are required to consult the Legal Department prior to offering or accepting any entertainment, meals, gifts, and travel expenses used to promote or discuss Company business.

### **5.3 Charitable Donations**

Charitable donations outside the United States can create significant anti-corruption risks if the donation directly or indirectly benefits a foreign government official or is a means of benefiting a private person. If an Owl Cyber Defense contribution to a non-U.S. organization has been otherwise approved by senior management, the Legal Department should be notified in order that an anti-corruption due diligence review on the transaction is performed.

### **5.4 Political Contributions**

Political contributions from Owl Cyber Defense are prohibited. Politically related contributions both inside and outside the United States may be illegal under applicable anti-corruption laws and present a particularly sensitive aspect of anti-corruption compliance. Accordingly, Owl Cyber Defense Representatives are not permitted to commit Owl Cyber Defense funds or Owl Cyber Defense resources to a source that would directly or indirectly benefit any political party, party officer, candidate for political office, or persons closely related to them. Owl Cyber Defense employees who receive requests for these types of political contributions or resources must immediately notify the Legal Department.

	<b>Title: Global Anti-Corruption Policy</b>	<b>Procedures</b>	<b>OWL-LG-PO-003</b>
	<b>Area: Legal Department</b>	<b>Initial Issue Date:</b>	<b>09/01/2022</b>
	<b>Approval: Counsel</b>	<b>Version:</b>	<b>01</b>
	<b>Page 8 of 11</b>	<b>Revision Date:</b>	<b>May 30, 2023</b>

## 5.5 Facilitation Payments

A Representative is prohibited from making any “facilitation” or “grease” payment, which is a payment made to a foreign government employee or official to facilitate or expedite a ministerial act or something that a government official was supposed to do anyway, such as processing a shipment, paperwork, or permit. Examples of services for which foreign government employees or officials may expect or request facilitation payments include: (a) obtaining customs clearance, permits, licenses or other official documents; (b) processing governmental papers (e.g., visas or work orders); (c) scheduling inspections associated with contract performance or inspections related to the transit of goods across country; and (d) loading and unloading cargo. (Note the foregoing does not include normal fees paid for a permit, license, or other certification fee, such as the fee paid for Passport.) While facilitation payments are not illegal under the United States Foreign Corrupt Practice Act (FCPA), they are illegal in many countries. You must contact the Legal Department immediately if you receive a request to make this type of payment. In rare instances, such payments may be authorized by Legal Counsel and in that event, will need to be accurately accounted for in company financial records.

## 5.6 Understand Local Laws

Owl Cyber Defense Representatives must be familiar with local anti-corruption laws prior to conducting business in a specific country. Each country has a unique set of anti-corruption laws, although most have a common prohibition on any type of offer or payment to a government official or commercial business prospect. Transparency International provides a valuable introductory resource that summarizes the anti-corruption laws of each country: <http://www.oas.org/juridico/english/Treaties/b-58.html>. In addition, the Legal Department will make resources immediately available to assist you with identifying, understanding, and complying with local anti-corruption laws.


## 5.7 Due Diligence

It is important that third-party due diligence encompass third parties contracted in both sales and supply channels. Contact Procurement/Contracts/Legal for assistance in determining that third parties are approved for contracting with Owl Cyber Defense. Though sales intermediaries (such as agents or distributors) may be more frequently abused than suppliers to relay corrupt payments, suppliers can likewise be used corruptly. As such, the request for a compliance check must be completed for all Non-U.S. Person third parties prior to engagement.

## 5.8 Mandatory Screening

As a U.S.-based company, Owl Cyber Defense is prohibited from employing or doing business with certain individuals, companies, and countries. For instance, certain individuals or companies may be on U.S.-blocked party lists or create specific anti-corruption restrictions. For this reason, it is necessary for every Non-U.S. Person third party (individual or company) to be formally screened before being engaged by Owl Cyber Defense.



	<b>Title: Global Anti-Corruption Policy</b>	<b>Procedures</b>	<b>OWL-LG-PO-003</b>
	<b>Area: Legal Department</b>	<b>Initial Issue Date:</b>	<b>09/01/2022</b>
	<b>Approval: Counsel</b>	<b>Version:</b>	<b>01</b>
	<b>Page 9 of 11</b>	<b>Revision Date:</b>	<b>May 30, 2023</b>

- Those contracting with Owl Cyber Defense (suppliers, subcontractors, vendors, clients, joint ventures, partners, etc.).
- Those acting on behalf of Owl Cyber Defense (contractor, agents, consultants, contract labor, representatives).

Mandatory Screening shall be performed before the party can be hired, consulted, or engaged.

### **5.9 Recordkeeping**

Owl Cyber Defense Representatives must submit a written record (receipts, invoices, etc.) for any payments, gifts, entertainment, travel, or other expenses provided to a private party or a government entity, government official, political party, or political party officer. These records must include reasonable detail to accurately reflect the nature of the transaction. Regardless of the type of transaction, all books and records must be complete and accurate. Owl Cyber Defense Representatives must never consent to the creation of false or misleading documents, including documents containing any misrepresentation or omission of payments.

Owl Cyber Defense’s Accounts Payable Department shall maintain best practice standards to ensure such expenses are authorized, properly recorded, and conform to generally accepted accounting principles. No record of payments, gifts, entertainment, or other such expenses can be kept “off book.” Examples of violations of this section include vague accounts such as “slush funds,” “petty cash,” “off-the-books” accounts, or payments to intermediaries without adequate justification and clear recordkeeping.

### **5.10 Anti-Corruption Reporting**


If an Owl Cyber Defense Representative becomes aware of or suspects any activity that is potentially a bribe or other corrupt act, the Representative must immediately contact the Legal Department. Owl Cyber Defense will not tolerate retaliation against any Owl Cyber Defense Representative who in good faith reports an issue or concern regarding compliance.

The Legal Department is available to all Owl Cyber Defense Representatives. If an Owl Cyber Defense Representative has any questions or concerns about any Owl Cyber Defense anti-corruption related issues, please contact the Legal Department.

### **5.11 Foreign Corrupt Practices Act (FCPA)**

The FCPA makes it unlawful to make payments to foreign government officials to assist in obtaining or retaining business.

Therefore, no Representatives have authority to violate the FCPA or any applicable anti-corruption law.

	<b>Title: Global Anti-Corruption Policy</b>	<b>Procedures</b>	<b>OWL-LG-PO-003</b>
	<b>Area: Legal Department</b>	<b>Initial Issue Date:</b>	<b>09/01/2022</b>
	<b>Approval: Counsel</b>	<b>Version:</b>	<b>01</b>
	<b>Page 10 of 11</b>	<b>Revision Date:</b>	<b>May 30, 2023</b>

The FCPA prohibits Representatives from corruptly paying, offering to pay, or giving anything of value to any Foreign Official in order to influence the Foreign Official in his or her official capacity, to induce the Foreign Official to do, or omit to do, an act in violation of his or her lawful duty, or to secure any improper advantage in order to assist in obtaining or retaining business for, or with, or directing business to, any person.

All Representatives are obligated to keep books, records, and accounts that accurately and fairly reflect all transactions and disposition of Company assets.

**5.12 Anti-Kickback Act of 1986**

It is an Owl Cyber Defense policy to fully comply with the Anti-Kickback Act of 1986 (41 U.S.C. 51-58) which prohibits offering, providing, attempting to provide, soliciting, accepting, or attempting to accept kickbacks in connection with U.S Government contracts and subcontracts and maintain “arm’s length” in all procurement transactions. Owl Cyber Defense Procurement/Contracts/Legal shall ensure that mandatory Anti-Kickback Act clauses are cited and incorporated into all subcontracts, purchase orders and other contractual awards issued by Owl Cyber Defense as required by FAR 52.203-7(c)(5). In part, the Act prohibits any person from:


- Providing, attempting to provide, or offering to provide any kickback;
- Soliciting, accepting, or attempting to accept any kickback; or
- Including, directly or indirectly, the amount of any kickback in the contract price charged by a subcontractor to a prime contractor or a higher tier subcontractor or in the contract price charged by a prime contractor to the United States.

A kickback need not be completed to fall within the ambit of the law. Even attempts to provide or receive a kickback are prohibited.

Each procurement decision must be awarded solely on the basis of quality, delivery, service, and/or price, and not on the promise of future business or the recognition of past business during the selection process.

**5.13 Conflicts of Law**

The expansion of laws prohibiting “official” and “commercial” bribery in countries where Owl Cyber Defense operates means that Representatives will encounter situations where local law appears to be inconsistent with the U.S. or other applicable national laws. If any potential conflict of law occurs, you must contact the Legal Department to ensure that Owl Cyber Defense takes the necessary steps to remain in full compliance with all applicable laws.

	<b>Title: Global Anti-Corruption Policy</b>	<b>Procedures</b>	<b>OWL-LG-PO-003</b>
	<b>Area: Legal Department</b>	<b>Initial Issue Date:</b>	<b>09/01/2022</b>
	<b>Approval: Counsel</b>	<b>Version:</b>	<b>01</b>
	<b>Page 11 of 11</b>	<b>Revision Date:</b>	<b>May 30, 2023</b>

#### 5.14 Audits and Reviews

Compliance with this Policy will be subject to an annual audit or review conducted by internal or other resources. Audits or reviews will examine compliance with applicable anti-corruption laws and mandatory directives set forth in this Policy.

### 6.0 **COMPLIANCE**

#### 6.1 *Code of Conduct: The Owl Cyber Commitment*

#### 6.2 Supplier/Reseller Code of Conduct

#### 6.3 Foreign Corruption Practices Act “FCPA” of 1977

<https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act>

#### 6.4 United Kingdom Bribery Act of 2010

<https://www.loc.gov/law/help/uk-bribery-act.php>

#### 6.5 Anti-Kickback Act of 1986

<https://www.justice.gov/jm/criminal-resource-manual-927-anti-kickback-act-1986>

#### 6.6 Federal Acquisition Regulations

<https://www.acquisition.gov/browse/index/far>

### 7.0 **REFERENCES and/or FORMS**

These documents are referenced in or applicable to this procedure.

### 8.0 **RECORD RETENTION AND DISPOSITION**

Record retention and disposition requirements will be in accordance with Owl Cyber Defense’s record retention policies and/or in accordance with specific contractual requirements.

### 9.0 **REVISION HISTORY**

Revision	Description of Change	Reason for Change	Update POC	Date
01	Remove Owl Proprietary Legend and add reference to a Supplier/Reseller Code of Conduct	This policy needs to be on our internet site	J. Reed	05/24/23