ESTRELLA IMMUNOPHARMA, INC.
CODE OF BUSINESS ETHICS AND CONDUCT

Effective as of September 29, 2023

1. Overview

Estrella Immunopharma, Inc. (the "***Company***") is committed to achieving the highest standards of professionalism and ethical conduct in its operations and activities and expects its employees, directors, and officers to conduct their business according to the highest ethical standards of conduct and to comply with all applicable laws, rules, and regulations.

The Company strives to create a culture of accountability and transparency. This Code of Business Ethics and Conduct ("***Policy***") is meant to assist employees, directors, and officers in making the right ethical and professional choices while conducting the Company's business. It is the Company's profound intent to create a culture of ethics in its daily operations through policies and procedures contained in this Policy, as well as other Company policies, along with education and training conducted by the Company from time to time.

An employee's failure to comply with this Policy may result in swift and immediate adverse employment consequences up to, and including, termination of employment. If circumstances warrant, the Company is obligated to notify appropriate law enforcement agencies. Illegal or unethical actions by anyone acting on the Company's behalf is unacceptable.

Additionally, as a public company, we have a responsibility to ensure that our filings with the Securities and Exchange Commission (the "***SEC***") and other public communications are timely and accurate. We expect each of our directors and officers and other employees to take this responsibility very seriously and act in accordance with the highest standards of personal and professional integrity in all aspects of their work related to our financial reporting.

Our board of directors (the "***Board of Directors***"), Chief Executive Officer, and Chief Financial Officer each have a special responsibility both to adhere to these principles themselves and to ensure that a culture exists throughout our organization as a whole, which ensures accurate and timely financial reporting. Because of these and other responsibilities, each of our directors, officers, and other employees is bound by this Policy.

2. Honest and Ethical Conduct

Company employees, officers, and directors must conduct their business affairs in an ethical, proper, and lawful manner. This means business must be conducted in compliance with all governing laws, regulations, and rules. But it also means that employees, directors, and officers must focus on doing what is right. Be mindful when discharging your duties and responsibilities so that your conduct is of the highest integrity. Employees, directors, and officers must not engage in questionable conduct or activities that may raise questions as to the Company's honesty, ethics, impartiality, or reputation or that may cause the Company reputational harm or embarrassment.

This additionally includes the ethical handling of actual or apparent conflicts of interest between personal and professional relationships. Deceit and subordination of principle are inconsistent with integrity. Each director, officer, and employee must (as applicable):

- engage in honest and ethical conduct, including the ethical handling of actual or apparent conflicts of interest between personal and professional relationships;
- produce full, fair, accurate, timely, and understandable disclosure in reports and documents that we file with or submit to the SEC and in other public communications we make;
- comply with applicable governmental laws, rules, and regulations;

- promptly report any illegal, improper, or unethical conduct or any violations of this Policy to the highest-ranking qualified officer of the Company or to the Audit Committee;

- act with integrity, including being honest and ethical while still maintaining the confidentiality of information where required or consistent with the Company's policies;

- observe both the form and the spirit of laws and governmental rules and regulations and accounting standards; and

- adhere to a high standard of business ethics.

Additionally, each officer, director, and employee (as applicable):

- Will not partake of activity that creates a conflict of interest for the Company and/or themselves personally. Personal investments or activities that create a conflict are prohibited.

- Will not seek personal gain through inappropriate use of the Company's nonpublic information or abuse of their position.

- Will protect the Company's information from improper disclosure and will follow all restrictions on use and disclosure of information.

- Will protect Company, customer, and third-party information, property, and assets and will use them only for appropriate Company-approved activities.

- Will not take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or unfair dealings.

- Will not either directly or indirectly, or allow others acting on the Company's behalf to, offer, make, or promise anything of value, or approve or authorize the giving of anything of value to an employee of any government, government-owned or -controlled political party, or international organization, or to a political party itself, in order to retain business to gain any improper advantage or benefit.

- Will not make payments, promises, or offers to expedite or facilitate any routine governmental action except as stated in the Anti-Bribery/Anti-Corruption section, and then only with the express approval of senior management.

- Will maintain complete and accurate books, records, and accounts in accurate detail that reflect all transactions including all expenses, disbursements, and receipts and the disposition of assets complying with accepted accounting rules and controls. Records shall be retained in accordance with the Company's Record Retention Policy.

- Will not retaliate against an employee who speaks up to report a concern.

Employees, directors, and officers must immediately report any actual or suspected violations of law, rules, regulations, or this Policy or any unethical conduct connected with the Company's business. Employees, directors, and officers are to seek guidance regarding any suspected code-of-conduct violations by sending an inquiry seeking guidance to the highest-ranking qualified officer of the Company.

The Company will not tolerate retaliation. Specifically, no employee, director, or officer of the Company may retaliate, threaten to retaliate, or cause any other person to retaliate or threaten to retaliate against any person who, in good faith, makes any compliance report, assists a colleague in making a report, or participates in any investigation.

The Company will endeavor to keep confidential the source of reports; however, disclosure may be required in certain circumstances under applicable laws or regulations, or made to facilitate an investigation or take appropriate remedial action. Employees should report concerns to their supervisor or the Company's designated personnel.

Reports involving directors and senior management may be made directly to the Audit Committee.

Nothing in this Policy in any way prohibits or is intended to restrict or impede you from exercising protected rights or otherwise disclosing information to law enforcement, regulatory, or administrative agencies as permitted by law.

3. Workplace Conduct

The Company is committed to providing its employees with a healthy, safe, fair, and productive work environment. All Company employees are expected to fully comply with the Company's policies and procedures and all applicable federal and state laws and regulations relating to health, safety, and the environment.

The Company believes diversity is an asset and will not tolerate discrimination or harassment of any kind. The Company strictly prohibits any kind of discrimination on the basis of race, color, veteran status, religion, disability, national origin, ethnicity, gender, sex, age, sexual orientation, gender identity, or any other characteristics protected by law. Sexual, verbal, physical, or visual harassment is prohibited.

Company employees should follow the Company reporting procedures for discrimination, harassment, and retaliation located in any Company policies that may be distributed to employees from time to time.

4. Anti-Bribery/Anti-Corruption

The Company is committed to complying with the highest ethical standards, including anti-bribery and anti-corruption obligations. As such, each director, officer, and employee shall not solicit, receive, give, or offer bribes, kickbacks, or inappropriate gifts or engage in other corrupt practices to obtain or maintain business or favors. These activities are illegal, and violations may be subject to fines, civil penalties, criminal prosecution, and/or imprisonment.

In particular, the Company's directors, officers, or employees shall not authorize, provide, promise, or offer to provide anything of value to a third party for the purpose or with the intent of improperly influencing his or her decisions or improperly performing his or her functions.

"***Bribery***" is defined as offering, promising, giving, receiving, or soliciting anything of value in order to influence how someone carries out a public, commercial, or legal duty.

"***Third party***" is defined as customers, vendors, suppliers, agents, distributors, developers, and local or foreign governments, agencies, political organizations, political candidates, etc.

This is especially important when providing anything of value to a "government official" or "foreign official." All gifts, entertainment, or other items of value that a Company employee may consider giving to a government or foreign official must be preapproved by the highest-ranking qualified officer of the Company. If approved, such payments are subject to strict record-keeping requirements.

It is also unlawful for companies to bribe or make corrupt payments to foreign government officials or any instrumentality of a foreign government. This includes foreign officials, any foreign political party or official, any candidate for foreign political office, or any person who knows that all or part of the payment will be offered, given, or promised to an individual falling within one of these categories. A "***foreign official***" is also defined as "any officer or employee of a foreign government or any department, agency, or instrumentality thereof or of a public international organization, or any person acting in an official capacity for or on behalf of any such government or department, agent or instrumentality, or for or on behalf of any such public international organization." This includes foreign state-owned and -controlled "business," including those operating in industries such as defense contracting and aerospace. Even low-level employees of these industries in foreign countries can be considered "foreign officials" under

anti-corruption/bribery statues. The Foreign Corrupt Practices Act ("***FCPA***") is a federal law that prohibits offering, giving, or promising to give anything of value to a non-U.S. government official to obtain or retain business, or obtain an improper business advantage. Accordingly, it is the Company's policy to keep accurate records of all transactions involving government officials.

Should the Company hire third parties or agents to perform services, these same procedures must be followed:

- Due diligence background check
- Written contract containing FCPA compliance, annual certification, termination for FCPA violation, or Company policy

Should a situation arise that may involve corruption, report the situation to the highest-ranking qualified officer of the Company immediately.

5. Gifts and Entertainment

Employees, officers, and directors are to avoid situations where gifts/entertainment appear to be a bribe or conflict of interest or could cause the Company reputational damage. It is never acceptable or appropriate to give personal benefits to a government official to bias a decision or to convey favor, and doing so for any reason is prohibited without alerting management in advance. The Company strictly follows laws prohibiting bribery, kickbacks, and corruption.

6. Conflicts of Interest

A "***conflict of interest***" arises when an individual's personal interest interferes or appears to interfere with the interests of the Company. A conflict of interest can arise when a director, officer, or employee takes actions or has personal interests that may make it difficult to perform his or her Company work objectively and effectively. For all employees and officers of the Company, any material transaction or relationship that could reasonably be expected to give rise to a conflict of interest should be discussed with the highest-ranking qualified officer of the Company. For all directors of the Company, any material transaction or relationship that could reasonably be expected to give rise to a conflict of interest should be discussed with the members of the Nominating and Corporate Governance Committee, who will act as arbiter in the matter. Interests in other companies, including potential competitors and suppliers, that are purely for investment purposes, are not significant to the individual, and do not include involvement in the management of the other entity, or where an otherwise questionable relationship is disclosed to the Company's Board of Directors and any necessary action is taken to ensure there will be no effect on the Company, are not considered conflicts unless otherwise determined by our Board of Directors. Fidelity or service to the Company should never be subordinated to or dependent on personal gain or advantage. Conflicts of interest should, whenever possible, be avoided. In most cases, anything that would constitute a conflict for a director, officer, or employee also would present a conflict if it is related to a member of his or her family.

Employees must report any actual or potential conflicts, including information necessary to determine whether a conflict exists. Participation in the following are a few examples of actual or potential conflicts:

- partnerships, directorships, trusteeships, and officers;
- acting as a consultant or otherwise performing work for a Company competitor, supplier of material, or service provider or a business that seeks to do business with the Company;
- investments in enterprises with which the Company does business or competes;
- giving a Company contract to a business you, your family, or your friend owns;
- compensation for services other than from the Company; and

- receiving loans, commissions, payments, or reimbursements for non–work-related expenses.

All disclosures must be written and directed to a supervisor. The highest-ranking qualified officer of the Company will review and determine whether there are conflicts and which, if any, can be resolved.

7. Antitrust

The Company must comply with anti-competition laws. These laws, also known as antitrust laws, protect competition by prohibiting anticompetitive behavior. Nonacceptable agreements with competitors include price fixing, bid rigging, market allocation, group boycotts, unlawful lying, anticompetitive information exchange, monopolization, and agreements that restrict supply. Employees are never to enter into these types of agreements. Entering into agreements or relationships that exchange competitively sensitive information with competitors is prohibited. Never share Company confidential or sensitive information with third parties. Of particular concern, do not share information related to operational and marketing strategies, costs, customers, or suppliers.

Entering agreements to restrict sales to certain customers or purchase from certain suppliers is also prohibited. This includes reaching agreements with competitors restricting where and/or to whom the Company will sell its products and/or purchase its materials.

The Company must make pricing decisions independently of competitors. Violations of the antitrust laws have both criminal and civil penalties for the Company and individuals.

8. Government Dealings and Political Activity

Company employees must ensure that information provided to government, regulatory, or agency officials is truthful and accurate whether provided orally, in writing, or otherwise. Should the matter involve a government investigation, other than a standard bid-award process, ensure records and information relevant to the inquiry are preserved. Never attempt to obstruct the investigation by concealing, altering, or destroying information, documents, or records that may be subject to the investigation.

The Company is not involved in any political activity. The Company will not make political contributions in cash or in kind. United States federal law prohibits the use of corporate funds, goods, or services to candidates for, or holders of, federal offices. Company policy prohibits all such contributions for any purpose to any office seeker or office holder anywhere. This also applies to Company support of campaign committees and political parties.

Company funds and assets may not be utilized for foreign or domestic political contribution or support without prior written consent. The Company will not reimburse personal political contributions.

We encourage employees to be involved in the political process as individuals, not as Company representatives. However, do not use the Company's time, property, or equipment to further personal political activities.

9. Cybersecurity and Digital Systems

All employees, directors, and officers of the Company must maintain strict security of Company information. Company information is the lifeblood of our business. Employees must keep all Company digital and cyber assets secure by adhering to security protocols administered by the Company's management.

Only authorized users who are current, active Company employees can access Company computers and network services including the Internet, email applications, and directories. Authorized users can only access digital assets needed to fulfill their job responsibilities. Company employees must keep their Company computer equipment secure and safe, including mobile equipment used for business, such as phones and laptops. Company employees must protect user IDs and passwords. Do not share user ID and password information or allow anyone else to use your assigned account. Company–issued computer equipment and related services such as email and Internet should be used primarily for Company business. Employees may utilize these systems for limited personal use. Immediately

report to the Company's management any suspected electronic security breach, computer virus, lost equipment, or lost information/documentation. Never transfer/copy Company confidential information into a memory stick unless permission is granted to do so. Never install or utilize unauthorized software.

Employees are not to make or retain any physical or electronic copies of any Company documents containing proprietary, confidential, or sensitive information belonging to the Company.

Never access, post, store, or publish pornographic images, sexually explicit content, or material that is terroristic, harassing, obscene, or abusive. The Company will not tolerate use of Company equipment, servers, or web access for the conduct of any illegal activities.

Employees must make sure to follow the Company's policies and procedures that are designed to protect the Company's systems, applications, networks, and assets from unauthorized access.

10. Protection of Company Assets

All employees are responsible for protecting the Company's assets from fraud, abuse, or waste. Company assets include physical property, intellectual Company property, business information, information, funds, corporate opportunities, operational and marketing strategies, costs, customers/potential customers, suppliers, and Company equipment. This information is both confidential and sensitive to the Company.

Intellectual Company property to be protected includes, but is not limited to, unpatented inventions, patented inventions, trademarks, designs, copyrighted materials, and trade secrets.

Intellectual property involves Company business information including, but not limited to, sales, marketing strategies, plans, and data; technical data and research; business proposals, strategies, and ideas; product development and design; software used by the Company; and customer strategies, marketing, and pricing.

The Company's most valuable assets are information gathered and developed, and its business operations. Some of this information is unknown to our competitors or the public and must be kept confidential.

Examples include:

- strategic business plans;
- information on pending sales, acquisitions, deals, or projects;
- vendor lists, customer information, pricing, and marketing information;
- personnel information;
- identified confidential information;
- proprietary data developed or held by the Company; and
- internal financial documents.

Employees must not disclose sensitive or nonpublic information with individuals outside the Company. Discussions between the Company and its lawyers may be privileged. Disclosure of those discussions to a third party may result in a waiver of the attorney–client privilege, resulting in potential harm to the Company.

Company assets are never to be used for a dishonest purpose, fraudulent act, or misappropriation. Company employees are prohibited from buying or selling a security on the basis of material, nonpublic information learned as a result of or through their position at the Company. Employees owe a duty of trust and confidence, or fiduciary duty, to the Company regarding information they learn through their Company employment. Employees may learn of

business opportunities through their association with the Company or their use of Company property, information, or position. These opportunities belong to the Company and must be disclosed to the Company. Employees may not disclose the opportunity to a third party or invest in that opportunity without the Company's prior written permission.

11. U.S. Sanctions

Sanctions programs are administered by the U.S. Department of Treasury Office of Foreign Assets Control ("***OFAC***"). The Company will not conduct business with countries identified on the OFAC list. Countries currently identified on the OFAC list include Cuba, Iran, Sudan, Syria, and North Korea. Employees must ensure that no Company transactions violate U.S. sanctions by looking out for facilitation or diversion of items to a sanctioned country. This includes use of an intermediary or third party in another country to facilitate a transaction with an OFAC-prohibited country.

12. Disclosure

Each director, officer, or employee—to the extent involved in the Company's disclosure process, including the Chief Executive Officer and the Chief Financial Officer (the "***Senior Financial Officers***")—is required to be familiar with the Company's disclosure controls and procedures and internal control over financial reporting, to the extent relevant to his or her area of responsibility, so that the Company's public reports and documents filed with the SEC comply in all material respects with the applicable federal securities laws and SEC rules. In addition, each such person having direct or supervisory authority regarding these SEC filings or the Company's other public communications concerning its general business, results, financial condition, and prospects should, to the extent appropriate within his or her area of responsibility, consult with other Company officers and employees and take other appropriate steps regarding these disclosures with the goal of making full, fair, accurate, timely, and understandable disclosure. Each director, officer, or employee, to the extent involved in the Company's disclosure process—including, without limitation, the Senior Financial Officers—must:

- familiarize himself or herself with the disclosure requirements applicable to the Company as well as the business and financial operations of the Company; and

- not knowingly misrepresent, or cause others to misrepresent, facts about the Company to others, whether within or outside the Company, including to the Company's independent auditors, governmental regulators, and self-regulatory organizations.

13. Compliance

It is the Company's policy to comply with all applicable laws, rules, and regulations. It is the personal responsibility of each employee, officer, and director to adhere to the standards and restrictions imposed by those laws, rules, and regulations in the performance of their duties for the Company, including those relating to accounting and auditing matters and insider trading. Generally, it is against Company policy for any individual to profit from undisclosed information relating to the Company or any other company in violation of insider-trading or other laws. Anyone who is aware of material nonpublic information relating to the Company, our customers, or other companies may not use the information to purchase or sell securities in violation of the federal securities laws. If you are uncertain about the legal rules involving your purchase or sale of any Company securities or any securities in companies that you are familiar with by virtue of your work for the Company, you should consult with the highest-ranking qualified officer of the Company before making any such purchase or sale. Other policies issued by the Company from time to time may also provide guidance as to certain of the laws, rules, and regulations that apply to the Company's activities.

14. Record-Keeping

As aforementioned, the Company's records and reports must be completed accurately and in compliance with accepted accounting rules and controls. This also applies to Company financial information. Books and records must be made and kept in reasonable detail and must accurately and fairly reflect transactions. Undisclosed or unrecorded funds or assets of the Company are not allowed. No entries will be made to intentionally conceal or disguise the true nature of any Company transaction. Misrepresentation or falsification of records or facts will not be tolerated. Any

reports, documents, patents, or data that the employee creates while working for the Company belongs to the Company. Without proper Company documentation and management authorization, never sell, transfer, or dispose of Company assets. Further, never destroy or remove records without obtaining permission. Relating to actual, pending, or threatened litigation or governmental investigations, never conceal, alter, transfer, or destroy Company information or property.

Any electronic or paper information is to be retained and/or destroyed only pursuant to the Company's policies on document management and applicable laws.

15. External Communications

Only authorized employees, consisting of the Company's management or its designees, shall respond to inquiries from the media, investors, brokers, and analysts.

16. Reporting, Accountability, No Retaliation

Reports of observed or suspected violations of this Policy will be investigated promptly, thoroughly, and in accordance with our legal obligations. Confidentiality is maintained to the fullest extent possible. We are all obliged to cooperate with investigations and provide complete, accurate, and truthful information. Violations of this Policy, which include failure to report potential violations by others, may be viewed as a severe disciplinary matter that may result in disciplinary action, up to and including termination of employment. Waivers of this Policy applicable to our directors and executive officers must be approved by our Board of Directors and will be publicly disclosed if granted. Waivers of this Policy to all other employees must be approved by the highest-ranking qualified officer of the Company.

It is a violation of this Policy to retaliate against any employee for good-faith reporting of violations of this code or cooperating in an investigation. Acts of retaliation may be considered misconduct that could result in disciplinary action.