GSI TECHNOLOGY, INC.

CODE OF CONDUCT AND POLICY REGARDING REPORTING OF POSSIBLE VIOLATIONS

As amended on October 27, 2026

1. Policy Statement

GSI is committed to operating with the highest level of business ethics in everything it does. That goal cannot be achieved unless you individually accept your responsibility to promote integrity and demonstrate the highest level of ethical conduct in all of your activities. Activities that may call into question the Company's reputation or integrity should be avoided. The Company understands that not every situation is black and white. The key to compliance with this Code is exercising good judgment. This means following the spirit of this Code and the law, doing the "right" thing and acting ethically even when the law is not specific. When you are faced with a business situation where you must determine the right thing to do, you should ask the following questions:

Am I following the spirit, as well as the letter, of any law or Company policy?

Would I want my actions reported on *60 Minutes*?

What would my family, friends or neighbors think of my actions?

Will there be any direct or indirect negative consequences for the Company?

Managers set an example for other employees and are often responsible for directing the actions of others. Every manager and supervisor is expected to take necessary actions to ensure compliance with this Code, to provide guidance and assist employees in resolving questions concerning the Code and to permit employees to express any concerns regarding compliance with this Code. No one has the authority to order another employee to act contrary to this Code.

2. Compliance with Laws and Regulations

The Company seeks to comply with both the letter and spirit of the laws and regulations in all countries in which it operates.

The Company is committed to full compliance with the laws and regulations of the cities, states and countries in which it operates. You must comply with all applicable laws, rules and regulations in performing your duties for the Company. Numerous federal, state and local laws and regulations define and establish obligations with which the Company, its employees and agents must comply. The following is a partial list of areas to which specific laws apply and every employee is required to consult the appropriate Company personnel to ensure compliance with these laws:

- Antitrust
- securities trading

- import/export matters
- taxation
- health and safety
- environmental matters
- anti-boycott
- mergers and acquisitions
- government contracting
- employment
- bribery and corruption
- domestic and international trade
- political activity
- privacy
- intellectual property (patents/copyright/trademark)

Under certain circumstances, local country law may establish requirements that differ from this Code. You are expected to comply with all local country laws in conducting the Company's business. If you violate these laws or regulations in performing your duties for the Company, you not only risk individual indictment, prosecution and penalties, and civil actions and penalties, you also subject the Company to the same risks and penalties. If you violate these laws in performing your duties for the Company, you may be subject to immediate disciplinary action, including possible termination of your employment or affiliation with the Company.

As explained below, you should always consult your manager or the Compliance Officer with any questions about the legality of your or your colleagues' conduct.

3. Full, Fair, Accurate, Timely and Understandable Disclosure

It is of paramount importance to the Company that all disclosure in reports and documents that the Company files with, or submits to, the Securities and Exchange Commission (the "SEC"), and in other public communications made by the Company is full, fair, accurate, timely and understandable. You must take all steps available to assist the Company in these responsibilities consistent with your role within the Company. In particular, you are required to provide prompt and accurate answers to all inquiries made to you in connection with the Company's preparation of its public reports and disclosure.

Any attempt to enter inaccurate or fraudulent information into the Company's accounting system will not be tolerated and will result in disciplinary action, up to and including termination of employment.

4. Special Ethics Obligations For Employees With Financial Reporting Responsibilities

The Company's Chief Executive Officer ("CEO"), Chief Financial Officer ("CFO"), controller and such other Company officers designated from time to time by the Audit Committee of the Board of Directors shall be deemed the Senior Officers of the Company. Senior Officers each bear a special responsibility for promoting integrity throughout the Company. Furthermore, the Senior Officers have a responsibility to foster a culture throughout the Company as a whole

that ensures the fair and timely reporting of the Company's results of operation and financial condition and other financial information.

Because of this special role, the Senior Officers are bound by the following Senior Officer Code of Ethics, and by accepting the Code of Business Conduct and Ethics each agrees that he or she will:

- Perform his or her duties in an honest and ethical manner;
- Handle all actual or apparent conflicts of interest between his or her personal and professional relationships in an ethical manner;
- Take all necessary actions to ensure full, fair, accurate, timely, and
- understandable disclosure in reports and documents that the Company files with, or submits to, government agencies and in other public communications;
- Comply with all applicable laws, rules and regulations of federal, state and local governments;
- Participate in the Open Door process, allow colleagues to raise issues, appropriately escalate those issues to complianceofficer@gsitechnology.com, and never undertake to self-investigate issues; and
- Proactively promote and be an example of ethical behavior in the work environment.

5. **Anti Trust**

You must follow all antitrust and fair competition laws in all jurisdictions in which GSI operates.

All of the Company's employees are required to comply with applicable antitrust laws and are prohibited from engaging in business practices that interfere with free and open competition among companies. Many business decisions raise antitrust issues, and even informal, unwritten business arrangements with competitors, suppliers, distributors or customers may unintentionally implicate antitrust laws. Additionally, violations of antitrust laws may result in severe civil and criminal consequences. Consequently, if there is any possibility that you are aware of or engaged in a behavior or enterprise that may implicate anti-trust laws, it is your responsibility to notify the Compliance Officer.

6. **Insider Trading and Prediction Markets**

You should never trade securities on the basis of confidential information acquired through your employment or fiduciary relationship with the Company.

You are prohibited under both federal law and Company policy from purchasing or selling Company stock, directly or indirectly, on the basis of material non-public information concerning the Company. Any person possessing material non-public information about the Company must not engage in transactions involving Company securities until this information has been released to the public. Generally, material information is that which would be expected to affect the investment decisions of a reasonable investor or the market price of the stock. You must also refrain from trading in the stock of other publicly held companies, such as existing or potential

customers or suppliers, on the basis of material confidential information obtained in the course of your employment or service as a director. It is also illegal to recommend a stock to (i.e., "tip") someone else on the basis of such information. If you have a question concerning appropriateness or legality of a particular securities transaction, consult with the Company's Compliance Officer. Officers, directors and certain other employees of the Company are subject to additional responsibilities under the Company's insider trading compliance policy, a copy of which has been provided to each officer, director and employee, and which can be obtained from the Compliance Officer.

In addition to prohibiting the use of inside information for the trading of securities, it is also GSI's policy to prohibit the use of inside or confidential information about GSI or any supplier, customer, or competitor to take positions on prediction markets, where an application "makes a market" for two parties to take positions against each other on a particular event. The law is still developing regarding the use of confidential information for this activity, but regardless of the legality of the activity, taking positions based on inside or confidential information learned as an employee at GSI is against company policy.

7. **Conflicts of Interest and Corporate Opportunities**

You must avoid any situation in which your personal interests conflict or even appear to conflict with the Company's interests. You owe a duty to the Company not to compromise the Company's legitimate interests and to advance such interests when the opportunity to do so arises in the course of your employment.

You shall perform your duties to the Company in an honest and ethical manner. You shall handle all actual or apparent conflicts of interest between your personal and professional relationships in an ethical manner.

You should avoid situations in which your personal, family or financial interests conflict or even appear to conflict with those of the Company. You may not engage in activities that compete with the Company or compromise its interests. You may not take for your own benefit opportunities discovered in the course of employment that you have reason to know would benefit the Company. The following are examples of actual or potential conflicts:

- you, or a member of your family, receive improper personal benefits as a result of your position in the Company;
- you use Company's property for your personal benefit; you engage in activities that interfere with your loyalty to the Company or your ability to perform Company duties or responsibilities effectively;
- you work simultaneously (whether as an employee or a consultant) for a competitor, customer or supplier;
- you, or a member of your family, have a financial interest in a customer, supplier, or competitor which is significant enough to cause divided loyalty with the Company or the appearance of divided loyalty (the significance of a financial interest depends on many factors, such as size of investment in relation to your income, net worth and/or financial needs, your potential to influence decisions that

could impact your interests, and the nature of the business or level of competition between the Company and the supplier, customer or competitor);

- you, or a member of your family, acquire an interest in property (such as real estate, patent or other intellectual property rights or securities) in which you have reason to know the Company has, or might have, a legitimate interest;
- you, or a member of your family, receive a loan or a guarantee of a loan from a customer, supplier or competitor (other than a loan from a financial institution made in the ordinary course of business and on an arm's-length basis);
- you divulge or use the Company's confidential information – such as financial data, customer information, or computer programs – for your own personal or business purposes;
- you make gifts or payments, or provide special favors, to customers, suppliers or competitors (or their immediate family members) with a value significant enough to cause the customer, supplier or competitor to make a purchase, or take or forego other action, which is beneficial to the Company and which the customer, supplier or competitor would not otherwise have taken; or
- you are given the right to buy stock in other companies or you receive cash or other payments in return for promoting the services of an advisor, such as an investment banker, to the Company.

Neither you, nor members of your immediate family, are permitted to solicit or accept valuable gifts, payments, special favors or other consideration from customers, suppliers or competitors. Any gifts may be accepted only on behalf of the Company with the approval of your manager and the Compliance Officer. Any gifts should be turned over to Employee Services for appropriate distribution. Any exchange of gifts must be conducted so that there is no appearance of impropriety. Gifts may be given only in compliance with the Foreign Corrupt Practices Act.

Conflicts are not always clear-cut. If you become aware of a conflict of the type described above or any other conflict, potential conflict, or have a question as to a potential conflict, you should consult with your manager or the Company's Compliance Officer and/or follow the procedures described in Sections 16 and 17of the Code. If you become involved in a situation that gives rise to an actual conflict, you must inform your supervisor or the Compliance Officer of the conflict.

8. **Confidentiality**

All confidential information concerning the Company obtained by you is the property of the Company and must be protected.

Confidential information includes all non-public information that might be of use to competitors, or harmful to the Company or its customers, if disclosed. You must maintain the confidentiality of such information entrusted to you by the Company, its customers and its suppliers, except when disclosure is authorized by the Company or required by law.

Examples of confidential information include, but are not limited to: the Company's trade secrets; business trends and projections; information about financial performance; new product or marketing plans; research and development ideas or information; manufacturing processes;

information about potential acquisitions, divestitures and investments; stock splits, public or private securities offerings or changes in dividend policies or amounts; significant personnel changes; and existing or potential major contracts, orders, suppliers, customers or finance sources or the loss thereof.

Your obligation with respect to confidential information extends beyond the workplace. In that respect, it applies to communications with your family members and continues to apply even after your employment or director relationship with the Company terminates.

9. Fair Dealing

Our goal is to conduct our business with integrity.

You should endeavor to deal honestly with the Company's customers, suppliers, competitors, and employees. Under federal and state laws, the Company is prohibited from engaging in unfair methods of competition, and unfair or deceptive acts and practices. You should not take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts, or any other unfair dealing.

Examples of prohibited conduct include, but are not limited to:

- bribery, kickbacks, or payoffs to induce business or breaches of contracts by others;
- acquiring a competitor's trade secrets through bribery or theft;
- making false, deceptive or disparaging claims or comparisons about competitors or their products or services; or
- mislabeling products or services.

10. Protection and Proper Use of Company Assets

You should endeavor to protect the Company's assets and ensure their proper use.

Company assets, both tangible and intangible, are to be used only for legitimate business purposes of the Company and only by authorized employees or consultants. Intangible assets include intellectual property such as trade secrets, patents, trademarks and copyrights, business, marketing and service plans, engineering and manufacturing ideas, designs, databases, Company records, salary information, and any unpublished financial data and reports. Unauthorized alteration, destruction, use, disclosure or distribution of Company assets violates Company policy and this Code. Theft or waste of, or carelessness in using, these assets have a direct adverse impact on the Company's operations and profitability and will not be tolerated.

The Company provides computers, voice mail, electronic mail (e-mail), and Internet access to certain employees for the purpose of achieving the Company's business objectives. As a result, the Company has the right to access, reprint, publish, or retain any information created, sent or contained in any of the Company's computers or e-mail systems of any Company machine. You may not use e-mail, the Internet or voice mail for any illegal purpose or in any manner that is contrary to the Company's policies or the standards embodied in this Code.

You should not make copies of, or resell or transfer copyrighted publications, including software, manuals, articles, books, and databases being used in the Company, that were created by another entity and licensed to the Company, unless you are authorized to do so under the applicable license agreement. In no event should you load or use, on any Company computer, any software, third party content or database without receiving the prior permission of the Management Information Systems Department to do so. You must refrain from transferring any data or information to any Company computer other than for Company use. You may use a handheld computing device or mobile phone in connection with your work for the Company, but must not use such device or phone to access, load or transfer content, software or data in violation of any applicable law or regulation or without the permission of the owner of such content, software or data. If you should have any question as to what is permitted in this regard, please consult with the Company's Senior Manager MIS.

11. Doing Business Internationally

We are committed to the highest business conduct standards worldwide.

We observe these business conduct standards worldwide, even at the risk of losing business. While no one can anticipate all the situations that may present challenges to you when doing business in the worldwide marketplace, the following guidelines always apply to you:

- Observe all laws and regulations, both U.S. and non-U.S., that apply to business abroad.
- Paying bribes to government officials is absolutely prohibited, even if those bribes are common practice, except for facilitating payments. You may not give, promise to give or authorize the giving to a foreign official, a foreign political party, or official thereof or any candidate for foreign political office any money or offer, gift, promise to give or authorize the giving of anything of value to influence any act or decision, to induce such official, party or candidate to do or omit to do any act in violation of the lawful duty of such official, party or candidate, or to induce such official, party or candidate to use his or her influence with a foreign government or agency to affect or influence any act or decision of such foreign government or agency.
- Do not cooperate with illegal boycotts.
- Observe all licensing requirements and the requirements of applicable import and export control laws.
- Do not enter into an agreement with an agent or consultant that relates to the Company's business outside the United States unless it has been approved by the Company.

The laws governing the Company's business in foreign countries are extensive and complex, and may be different from those in the United States. No Company services or products should be offered in any new country without prior approval, and then only in accordance with the applicable local country's regulations and requirements.

12. Import and Export Regulation/Trade Compliance

We are subject to the import and export laws and regulations of the United States and certain foreign governments that govern the international transfer of our products and services, as well as our technology, information and ideas.

Under U.S. law, no technology may be exported without the proper government export licenses and documentation. Exports of technology include not only technology shipped via freight, but also technology that is hand-carried (employees traveling overseas), sent via courier services or U.S. mail, electronically transmitted, and/or disclosed to foreign nationals in the United States or abroad. "Technology" is defined as hardware, software, technical documentation, product specifications, technical data, etc.

It is your responsibility to ensure that proper documentation accompanies each export or disclosure. Failure to export or re-export without the proper export license or documentation can jeopardize the Company's compliance with U.S. export laws, as well as those laws of foreign countries. Non-compliance can result in denial of export privileges, criminal penalties, seizure of commodities, and fines to the Company and each of us.

It is the Company's policy to comply fully with all applicable U.S. and foreign laws controlling the export and re-export of products, technology (including software) and services. You must exercise the necessary diligence to ensure that the Company complies with all applicable U.S. and foreign government regulations regarding exports.

13. Antiboycott Compliance

We must comply with antiboycott regulations enacted by the United States government.

These regulations make it unlawful for U.S. persons to participate in any activity that could have the effect of promoting or supporting a boycott or restrictive trade practice of another country against customers or suppliers located in a country friendly to the U.S. or against a U.S. person, firm or corporation. Boycott issues arise most frequently in connection with the Arab boycott of Israel. Prohibited actions include, but are not limited to, furnishing information about business relationships with boycotted countries, or information about race, religion, sex or national origin. Any request to participate in such activity should be

immediately reported to the Compliance Officer.

14. Government Contracting

We are subject to detailed laws and regulations that govern virtually every aspect of doing business with the U.S. government and its agencies.

You should seek to adhere to the highest standards of honesty and integrity in their relations with government officials and employees. Activities that might be permitted when working with the private sector may be improper or even illegal when a national or local government is the customer. For example, you should observe the following principles when bidding or performing government contracts:

- Do not offer or provide meals, transportation, gifts or other consideration to government employees except as permitted under applicable law and Company policy.
- Obey the regulations governing current and post-government employee conflicts of interests. Obtain all appropriate government approvals prior to recruiting or hiring current or former government employees.
- Obtain appropriate licenses prior to exporting or even discussing certain technologies with citizens of other countries.
- Obey any requirements that may restrict access to source selection or competitive information.
- If you deal with government representatives, you are responsible for knowing and obeying the laws and regulations applicable to doing business with the U.S. government.

15. Privacy

We comply with the privacy laws of the states and countries in which GSI operates to protect both employee, customer, and vendor privacy.

Whenever you are engaged in an activity where you may collect, store, or process sensitive personal data from our employees, customers, or other stakeholders, you should take the upmost precautions to protect that data. Many jurisdictions that GSI operates in have specific laws and regulations governing how companies must protect sensitive data. In all cases GSI adheres to those laws and regulations. If your role at GSI requires you to collect, store, process, or analyze sensitive personal data, it is your responsibility to ensure that the company does so in a lawful and appropriate manner. If you have questions about how sensitive personal data should be handled in a particular state or country, you can reach out to privacy@gsitechnology.com.

16. Reporting Violations of Company Policies and Receipt of Complaints Regarding Financial Reporting or Accounting Issues

It is your obligation as a GSI employee to report any violation or suspected violation of this Code, company policy, or the law to the appropriate Company personnel or via the Company's anonymous and confidential reporting procedures

As part of GSI's commitment to acting with the upmost business integrity, we rely on you, the employee of GSI, to raise issues about potential violations of the Code of Conduct, company policy, or the law. Without you, GSI may never know if a significant violation has occurred that could put the company at serious risk.

The company does not ask you, the employee, to investigate or determine what type of risk the issue might present. In other words, you do not need to know if the issue presents a human resource issue, a legal issue, a financial reporting issue, a regulatory issue, or an issue that might involve one or more of these things. You just need to know to report the issue using one of the channels set forth below.

The company provides numerous ways for you to report an issue:

- You may report any issue to GSI's Compliance Officer;
- You may report any issue via the Open Door process, as outlined in the Employee Handbook, to your direct supervisor or any GSI manager, or the Personal Administrator. Supervisors or managers who receive any report of a suspected violation of company policy or the law must report the matter to the Compliance Officer using the following email complianceofficer@gsitechnology.com; and
- You may report any issue directly to the Chair of the Board Audit Committee at auditcommitteechair@gsitechnology.com.

If you wish to report any such matters anonymously, you may do so as follows:

- Contact: http://www.openboard.info/GSIT/
- Calling toll free **1-866-240-8421** our Compliance Hotline.
- Mail a description of the suspected violation or other complaint or concern to:

  Compliance Officer
  GSI Technology, Inc.
  1213 Elko Drive
  Sunnyvale, CA 94089

  or

  Audit Committee Chair
  GSI Technology, Inc.
  1213 Elko Drive
  Sunnyvale, CA 94089

- Please note, anonymous reporting is available in all countries where it is permitted under local law. In countries where it is prohibited, GSI cannot make that option available.
- In all cases in which you report a suspected violation, the Company will attempt to keep its discussions with you confidential to the extent reasonably possible. In the course of its investigation, the Company may find it necessary to share information with others on a "need to know" basis.
- If you become aware of a suspected violation, don't try to investigate it or resolve it on your own.
- Use common sense and good judgment. You are expected to become familiar with and to understand the requirements of this Code. Prompt disclosure to the appropriate parties is vital to ensuring a thorough and timely investigation and resolution. The circumstances should be reviewed by appropriate personnel as promptly as possible, and a delay may affect the results of any investigation. A violation of this Code, any company policy, or of applicable laws and/or governmental regulations is a serious matter and could have legal implications. Allegations of such behavior are not taken lightly and should not be made to

embarrass someone or put him or her in a false light. Reports of suspected violations should always be made in good faith.

- When an alleged violation of this Code, any company policy, applicable laws and/or governmental regulations is reported, the Company will take appropriate action in accordance with the compliance procedures outlined in Section 1 of the Code. In all cases, GSI will evaluate issues as they are raised and determine whether they need to be handled by arms-length, independent investigators.
- All GSI employees are expected to cooperate in internal investigations of alleged misconduct or violations of this Code or of applicable laws or regulations.
- It is Company policy that there be no retaliation against any person who provides information in good faith to a Company or law enforcement official concerning a possible violation of any law, regulation or Company policy, including this Code. Persons who retaliate may be subject to civil, criminal and administrative penalties, as well as disciplinary action, up to and including termination of employment.

17. **Compliance Procedures**

The Company has established this Code as part of its overall policies and procedures. To the extent that other Company policies and procedures conflict with this Code, you should follow this Code. This Code applies to all Company directors and Company employees, including all officers, in all locations.

This Code is based on the Company's core values, good business practices and applicable law. The existence of a Code, however, does not ensure that directors, officers, and employees will comply with it or act in a legal and ethical manner. To achieve optimal legal and ethical behavior, the individuals subject to the Code must know and understand the Code as it applies to them and as it applies to others. You must champion the Code and assist others in knowing and understanding it.

- Compliance. You are expected to become familiar with and understand the requirements of this Code. Most importantly, you must comply with it.

- CEO Responsibility. The Company's CEO shall be responsible for ensuring that this Code is established and effectively communicated to all employees, officers, and directors. Although the day-to-day compliance issues will be the responsibility of the Company's managers, the CEO has ultimate accountability with respect to the overall implementation of and successful compliance with this Code.

- Corporate Compliance Management. The CEO shall select an employee to act as the Corporate Compliance Officer. The Corporate Compliance Officer is currently Douglas Schirle, the Company's Chief Financial Officer. The Compliance Officer's charter is to ensure communication, training, monitoring, and overall compliance with this Code. The Compliance Officer will, with the assistance and cooperation of the Company's officers, directors, and managers, foster an atmosphere where employees are comfortable in communicating and/or reporting concerns and possible Code violations.

- Internal Reporting of Violations. The Company's efforts to ensure observance of, and adherence to, the goals and policies outlined in this Code mandate that all employees, officers, and directors of the Company report suspected violations in accordance with Section 16 of this Code.

- Screening of Employees. The Company shall exercise due diligence when hiring and promoting employees and, in particular, when conducting an employment search for a position involving the exercise of substantial discretionary authority, such as a member of the executive team, a senior management position or an employee with financial management responsibilities. The Company shall make reasonable inquiries into the background of each individual who is a candidate for such a position. All such inquiries shall be made in accordance with applicable law and good business practice.

- Access to the Code. The Company shall ensure that employees, officers, and directors may access this Code on the Company's website. In addition, each current employee will be provided with a copy of this Code. New employees will receive a copy of this Code as part of their new hire information. From time to time, the Company will sponsor employee training programs in which this Code and other Company policies and procedures will be discussed.

- Managerial Responsibility. The officers of the Company shall be accountable for ensuring all of the Company's managers have reviewed this Code. In turn, the Company's managers with supervisory responsibilities are accountable for reviewing this Code with their direct reports. Managers are the "go to" persons for employee questions and concerns relating to this Code, especially in the event of a potential violation. Managers or supervisors will immediately report any violations or allegations of violations raised through the Open Door Process described in the Employee Handbook or learned about through other means to Compliance Officer by using complianceofficer@gsitechnology.com. Managers will work with Compliance Officer in assessing areas of concern, potential violations, any needs for enhancement of this Code, or remedial actions to affect this Code's policies and overall compliance with this Code and other related policies. Managers should never investigate potential violations of company policy or the law on their own.

- Auditing. As needed the Audit Committee working with the Compliance Officer will engage an internal audit team to audit the Company's compliance with this Code.

- Internal Investigation. When an alleged violation of the Code is reported, the Compliance Officer shall take prompt and appropriate action in accordance with the law and regulations and otherwise consistent with good business practice. If the suspected violation appears to involve either a possible violation of law or an issue of significant corporate interest, or if the report involves a complaint or concern of any person, whether an employee, a shareholder or another interested person regarding the Company's financial disclosure, internal accounting controls, questionable auditing or accounting matters or practices or other issues relating to

the Company's accounting or auditing, then the manager or investigator should immediately notify the Compliance Officer, who, in turn, shall notify the Chair of the Audit Committee. If a suspected violation involves any director or executive officer or if the suspected violation concerns any fraud, whether or not material, involving management or other employees who have a significant role in the Company's internal controls, any person who received such report should immediately report the alleged violation to through the channels set forth in section 16 of the Code. As set forth in Section 16, the Compliance Officer and Chair of the Audit Committee will receive reports of suspected violations. The Compliance Officer, or the Chair of the Audit Committee, if the Compliance Officer should ever be implicated in an allegation or be unavailable, shall assess the situation and determine the appropriate course of action. At a point in the process consistent with the need to conduct a proper investigation, any person who is suspected of a violation shall be apprised of the alleged violation and shall have an opportunity to provide a response to the investigator.

- Disciplinary Actions. Subject to the following sentence, the Compliance Officer, after consultation with the Administrator/Human Resources Manager, and legal counsel, shall be responsible for implementing the appropriate disciplinary action in accordance with the Company's policies and procedures for any employee who is found to have violated the Code, policy, or the law. If a violation has been reported directly to the Audit Committee or another committee of the Board, that Committee shall be responsible for determining appropriate disciplinary action. Any violation of applicable law or any deviation from the standards embodied in this Code will result in disciplinary action, up to and including termination of employment. Any employee engaged in the exercise of substantial discretionary authority, including any Senior Officer, who is found to have engaged in a violation of law or unethical conduct in connection with the performance of his or her duties for the Company, shall be removed from his or her position and not assigned to any other position involving the exercise of substantial discretionary authority. In addition to imposing discipline upon employees involved in non-compliant conduct, the Company also will impose discipline, as appropriate, upon an employee's supervisor, if any, who directs or approves such employees' improper actions, or is aware of those actions but does not act appropriately to correct them, and upon other individuals who fail to report known non-compliant conduct.

- Retention of Reports and Complaints. All reports and complaints made to or received by the Compliance Officer or the Chair of the Audit Committee shall be logged into a record maintained for this purpose by the Compliance Officer and this record of such report shall be retained for five (5) years.

- Voluntary Disclosure. The Compliance Officer shall be responsible for evaluating all substantiated violations of company policy or the law for potential disclosure under the US Department of Justice Corporate Enforcement Policy or other disclosure policies by relevant regulators in the US or in other countries. In no way does this preclude direct disclosure to appropriate authorities by GSI employees or stakeholders.

- Corrective Actions. Subject to the following sentence, in the event of a violation of the Code, the manager and the Compliance Officer should assess the situation to determine whether the violation demonstrates a problem that requires remedial action as to Company policies and procedures. If a violation has been directly reported to the Audit Committee or another committee of the Board, that committee shall be responsible for determining appropriate remedial or corrective actions. Such corrective action may include providing revised public disclosure, retraining Company employees, modifying Company policies and procedures, improving monitoring of compliance under existing procedures and other action necessary to detect similar non-compliant conduct and prevent it from occurring in the future. Such corrective action shall be documented and clear accountability will be assigned to ensure all corrective actions are implemented.

18. Publication of the Code of Business Conduct and Ethics; Amendments and Waivers of the Code of Business Conduct and Ethics

The most current version of this Code will be posted and maintained on the Company's website and filed as an exhibit to the Company's Annual Report on Form 10-K. The Company's Annual Report on Form 10-K shall disclose that the Code is maintained on the website and shall disclose that substantive amendments and waivers will also be posted on the company's website.

Any substantive amendment or waiver of this Code (i.e., a material departure from the requirements of any provision) particularly applicable to or directed at executive officers or directors may be made only after approval by the Board of Directors and will be disclosed within four (4) business days of such action (a) on the Company's website for a period of not less than twelve (12) months and (b) in a Form 8-K filed with the Securities and Exchange Commission. Such disclosure shall include the reasons for any waiver. The Company shall retain the disclosure relating to any such amendment or waiver for less than five (5) years.

CERTIFICATION

The undersigned certifies that the undersigned has read, understands and agrees to comply with the Code of Conduct of GSI Technology, Inc. (the "Company"). The undersigned agrees that the undersigned will be subject to sanctions, including, as to employees of the Company, termination of employment, that may be imposed by the Company, in its discretion, for violation of the Company's policy.

Employee:

_____

Signature

_____

Printed Name

_____

Date