



GTY TECHNOLOGY

GTY TECHNOLOGY HOLDINGS INC.

CODE OF BUSINESS CONDUCT AND ETHICS FOR EMPLOYEES, EXECUTIVE OFFICERS AND DIRECTORS

Introduction

GTY Technology Holdings Inc. (the “*Company*”) is committed to maintaining the highest standards of business conduct and ethics. This Code of Business Conduct and Ethics (the “*Code*”) reflects the business practices and principles of behavior that support this commitment. The Company expects every employee, officer and director to read and understand the Code and its application to the performance of his or her business responsibilities. This Code applies to all employees, members of the Board of Directors (the “*Board*”), officers and consultants of the Company.

Directors, officers (of both the Company and its subsidiaries) and other managers are expected to develop in employees a sense of commitment to the spirit, as well as the letter, of the Code. The Chief Executive Officer of each subsidiary of the Company (each, a “Subsidiary CEO”) is also expected to ensure that all agents and contractors conform to Code standards when working for or on behalf of the Company. This Code supersedes all other codes of conduct, policies, procedures, instructions, practices, rules or written or verbal representations to the extent that they are inconsistent with this Code. However, nothing in this Code otherwise alters the at-will employment policy of the Company, where such policies are permissible by law. The Company is committed to continuously reviewing and updating its policies and procedures. This Code, therefore, is subject to modification.

This Code cannot possibly describe every practice or principle related to honest and ethical conduct. The Code addresses conduct that is particularly important to proper dealings with the people and entities with which the Company interacts but reflects only a part of the Company’s commitment. From time to time the Company may adopt additional policies and procedures with which the Company’s employees, officers and directors are expected to comply, if applicable to them. However, it is the responsibility of each employee to apply common sense, together with his or her own highest personal ethical standards, in making business decisions where there is no stated guideline in the Code.

Action by members of your family, significant others or other persons who live in your household (referred to in the Code as “*family members*”) also may potentially result in ethical issues to the extent that they involve the Company’s business. For example, acceptance of inappropriate gifts by a family member from one of the Company’s suppliers could create a conflict of interest and result in a Code violation attributable to you. Consequently, in complying with the

Code, you should consider not only your own conduct, but also that of your family members, significant others and other persons who live in your household.

You should not hesitate to ask questions about whether any conduct may violate the Code, voice concerns or clarify gray areas. Section 18 below details the compliance resources available to you. In addition, you should be alert to possible violations of the Code by others and report suspected violations, without any fear of any form of retaliation, as further described in Section 18 below. Violations of the Code will not be tolerated. Any employee who violates the standards in the Code may be subject to disciplinary action, which, depending on the nature of the violation and the history of the employee, may range from a warning or reprimand to and including termination of employment and, in appropriate cases, civil legal action or referral for regulatory or criminal prosecution.

1. Honest and Ethical Conduct

It is the policy of the Company to promote high standards of integrity by conducting the Company's affairs in an honest and ethical manner. The integrity and reputation of the Company depends on the honesty, fairness and integrity brought to the job by each person associated with the Company. Unyielding personal integrity is the foundation of corporate integrity.

2. Legal Compliance

Obedying the law, both in letter and in spirit, is the foundation of this Code. The Company's success depends upon each employee's operating within legal guidelines and cooperating with local, national and international authorities. The Company expects employees to understand the legal and regulatory requirements applicable to their business units and areas of responsibility. While the Company does not expect you to memorize every detail of these laws, rules and regulations, the Company wants you to be able to determine when to seek advice from others. If you do have a question in the area of legal compliance, it is important that you not hesitate to seek answers from your Subsidiary CEO or the Chief Operating Officer of the Company (as further described in Section 18 below).

Disregard of the law will not be tolerated. Violation of domestic or foreign laws, rules and regulations may subject an individual, as well as the Company, to civil and/or criminal penalties.

You should be aware that conduct and records, including emails, are subject to internal and external audits, and to discovery by third parties in the event of a government investigation or civil litigation. It is in everyone's best interests to know and comply with the Company's legal and ethical obligations.

3. Government Investigations

It is the Company's policy to cooperate with government investigations and give government investigators the full measure of assistance to which they are entitled, consistent with the safeguards that the law has established for the benefit of persons under investigation. Such persons should have the opportunity to be adequately represented in such investigations by legal counsel. This Code sets forth the standards that employees, directors, officers and consultants of the Company should follow if such person is contacted by a government investigator or law enforcement official.

If a government investigator or agency contacts an employee, director, officer or consultant of the Company seeking information or access to the Company's records or facilities, such person should politely inform the investigator or agency that the Company's policy is generally one of cooperation, but that such person must obtain clearance from the Chief Operating Officer before furnishing such information or access, unless management has established written policies relating to the agency and type of inspection that is being requested (*e.g.*, OSHA).

If employees are approached at home or at work by a government regulatory official or law enforcement officer investigating the Company, its operations or business practices, the employee can insist that any interview take place at an office or another location away from the employee's home. Employees should also know that no government official or law enforcement officer can require the employee to give information without the opportunity to consult with an attorney.

Under no circumstances should an employee lie or make any misleading statements to any government investigator or law enforcement official, attempt or cause any other employee or any other person to fail to provide information to any government investigator, or provide any false or misleading information.

If an employee obtains information that would lead the employee to believe that a government investigation is underway, or if an employee is contacted by any government regulatory or law enforcement official regarding the Company, the employee should contact the Chief Operating Officer.

4. Insider Trading

Directors, officers or employees who have confidential (or "*inside*") information are not permitted to use or share that information for purposes of trading in the Company's securities or for any other purpose except to conduct the Company's business. All non-public information about the Company or about companies with which the Company does business is considered confidential information. To use material non-public information in connection with buying or selling securities, including "tipping" others who might make an investment decision on the basis of this information, is not only unethical, it is illegal. Employees must exercise the utmost care when handling material inside information. The Company has adopted a Policy Regarding Insider Trading and Dissemination of Inside Information which every director, officer and employee should carefully review.

5. Certain Laws

Antitrust

Antitrust laws are designed to protect the competitive process. These laws are based on the premise that the public interest is best served by vigorous competition and will suffer from illegal agreements or collusion among competitors. Antitrust laws generally prohibit:

- agreements, formal or informal, with competitors that harm competition or customers, including price fixing and allocations of customers, territories or contracts;
- agreements, formal or informal, that establish or fix the price at which a customer may resell a product; and

- the acquisition or maintenance of a monopoly or attempted monopoly through anticompetitive conduct.

Certain kinds of information, such as pricing, should not be exchanged with competitors, regardless of how innocent or casual the exchange may be and regardless of the setting, whether business or social.

Antitrust laws impose severe penalties for certain types of violations, including criminal penalties and potential fines and damages of millions of dollars, which may be tripled under certain circumstances. Understanding the requirements of antitrust and unfair competition laws of the various jurisdictions where the Company does business can be difficult, and you are urged to seek assistance from your Subsidiary CEO or the Chief Operating Officer (as further described in Section 18 below) whenever you have a question relating to these laws.

International Business Laws

Our employees are expected to comply with the applicable laws in all countries to which they travel, in which they operate and where the Company otherwise does business, including laws prohibiting bribery, corruption or the conduct of business with specified individuals, companies or countries. The fact that in some countries certain laws are not enforced or that violation of those laws is not subject to public criticism will not be accepted as an excuse for noncompliance. In addition, the Company expects employees to comply with United States laws, rules and regulations governing the conduct of business by its citizens and corporations outside the U.S.

If you have a question as to whether an activity is restricted or prohibited, seek assistance before taking any action, including giving any verbal assurances that might be regulated by international laws.

6. Conflicts of Interest

The Company respects the rights of the Company's employees to manage their personal affairs and investments and does not wish to impinge on their personal lives. At the same time, employees should avoid conflicts of interest that occur when their personal interests may interfere in any way with the performance of their duties or the best interests of the Company. A conflicting personal interest could result from an expectation of personal gain now or in the future or from a need to satisfy a prior or concurrent personal obligation. The Company expects employees to be free from influences that conflict with the best interests of the Company or might deprive the Company of their undivided loyalty in business dealings. Even the appearance of a conflict of interest where none actually exists can be damaging and should be avoided. Whether or not a conflict of interest exists or will exist can be unclear. Conflicts of interest are prohibited unless specifically authorized as described below.

If you have any questions about a potential conflict or if you become aware of an actual or potential conflict, and you are not an officer of the Company or member of the Board, you should discuss the matter with your Subsidiary CEO or the Chief Operating Officer (as further described in Section 18 below). Subsidiary CEOs may not authorize conflict of interest matters without first seeking the approval of the Chief Operating Officer and providing the Chief Operating Officer with a written description of the activity. If the Subsidiary CEO is involved in the potential or actual conflict, you should discuss the matter directly with the Chief Operating Officer. Officers

and members of the Board may seek authorization from the Board. Factors that may be considered in evaluating a potential conflict of interest are, among others:

- whether it may interfere with the employee's job performance, responsibilities or morale;
- whether the employee has access to confidential information;
- whether it may interfere with the job performance, responsibilities or morale of others within the organization;
- any potential adverse or beneficial impact on the Company's business;
- any potential adverse or beneficial impact on the Company's relationships with the Company's customers or suppliers or other service providers;
- whether it would enhance or support a competitor's position;
- the extent to which it would result in financial or other benefit (direct or indirect) to the employee;
- the extent to which it would result in financial or other benefit (direct or indirect) to one of the Company's customers, suppliers or other service providers; and
- the extent to which it would appear improper to an outside observer.

Although no list can include every possible situation in which a conflict of interest could arise, the following are examples of situations that may, depending on the facts and circumstances, involve conflicts of interests:

- *Employment by (including consulting for) or service on the board of directors of a competitor, customer or supplier or other service provider.* Activity that enhances or supports the position of a competitor to the detriment of the Company is prohibited, including employment by or service on the board of a competitor. Employment by or service on the board of directors of a customer or supplier or other service provider is generally discouraged and you must seek authorization in advance if you plan to take such a position.
- *Owning, directly or indirectly, a significant financial interest in any entity that does business, seeks to do business or competes with the Company.* In addition to the factors described above, persons evaluating ownership in other entities for conflicts of interest will consider: the size and nature of the investment; the nature of the relationship between the other entity and the Company; the employee's access to confidential information; and the employee's ability to influence the Company's decisions. If you would like to acquire a financial interest of that kind, you must seek approval in advance.

- *Soliciting or accepting gifts, favors, loans or preferential treatment from any person or entity that does business or seeks to do business with the Company.* See Section 12 below for further discussion of the issues involved in this type of conflict.
- *Soliciting contributions to any charity or for any political candidate from any person or entity that does business or seeks to do business with the Company.*
- *Taking personal advantage of corporate opportunities.* See Section 8 below for further discussion of the issues involved in this type of conflict.
- *Moonlighting without permission.*
- *Conducting the Company's business transactions with your family member or a business in which you have a significant financial interest.* Material related-party transactions involving any executive officer or director, 5% shareholder or member of their respective immediate families are subject to the Company's Related Party Transaction Policies and Procedures.
- *Exercising supervisory or other authority on behalf of the Company over a co-worker who is also a family member.* The employee's Subsidiary CEO and/or the Chief Operating Officer will consult with the Human Resources Department to assess the advisability of reassignment.

Loans to, or guarantees of obligations of, employees or their family members by the Company could constitute an improper personal benefit to the recipients of these loans or guarantees, depending on the facts and circumstances. Some loans are expressly prohibited by law, and applicable law requires that the Board approve all loans and guarantees to employees. As a result, all loans and guarantees by the Company must be approved in advance by the Board.

7. Treatment with Fairness and Respect

You are critical to the success of the Company, and the Company's policy is to treat you with fairness and respect. The Company is an equal opportunity employer. The Company does not tolerate discrimination against applicants or employees based on race, religion, gender, age, marital status, national origin, sexual orientation, citizenship status or other protected characteristics or disability. The Company prohibits discrimination in decisions concerning recruitment, hiring, compensation, benefits, training, termination, promotions or any other condition of employment or career development. The Company is committed to providing a work environment that is free from discrimination and/or harassment. The Company will not tolerate the use of discriminatory slurs; unwelcome, unsolicited sexual advances or harassment; or any other remarks, jokes or conduct that create or foster an offensive or hostile work environment. Each person, at every level of the organization, must act with respect toward customers, coworkers and outside firms.

8. Corporate Opportunities

You may not take personal advantage of opportunities for the Company that are presented to you or discovered by you as a result of your position with the Company or through your use of corporate property or information, unless authorized by your Subsidiary CEO, the Chief Operating Officer or the Board. Even opportunities that are acquired privately by you may be questionable if

they are related to the Company's existing or proposed lines of business. Participation in an investment or outside business opportunity that is directly related to the Company's lines of business must be preapproved. You may not use your position with the Company or corporate property or information for improper personal gain, nor should you compete with the Company in any way.

9. Maintenance of Corporate Books, Records, Documents and Accounts; Financial Integrity; Public Reporting

The integrity of the Company's records and public disclosure depends upon the validity, accuracy and completeness of the information supporting the entries to the Company's books of account. Therefore, the Company's corporate and business records should be completed accurately and honestly.

The making of false or misleading entries, whether they relate to financial results or otherwise, is strictly prohibited. The Company's records serve as a basis for managing its business and are important in meeting its obligations to customers, suppliers, creditors, employees and others with whom the Company does business. As a result, it is important that the Company's books, records and accounts accurately and fairly reflect, in reasonable detail, the Company's assets, liabilities, revenues, costs and expenses, as well as all transactions and changes in assets and liabilities. The Company requires that:

- no entry be made in the Company's books and records that intentionally hides or disguises the nature of any transaction or of any of the Company's liabilities, or misclassifies any transactions as to accounts or accounting periods;
- transactions be supported by appropriate documentation;
- the terms of sales and other commercial transactions be reflected accurately in the documentation for those transactions and all such documentation be reflected accurately in the Company's books and records;
- employees comply with the Company's system of internal controls; and
- no cash or other assets be maintained for any purpose in any unrecorded or "off-the-books" fund.

The Company's accounting records are also relied upon to produce reports for its management, stockholders and creditors, as well as governmental agencies. In particular, the Company relies upon its accounting and other business and corporate records in preparing periodic and current reports that it files with the United States Securities and Exchange Commission (the "*SEC*"). Securities laws require that these reports provide full, fair, accurate, timely and understandable disclosure and fairly present the Company's financial condition and results of operations. Employees who collect, provide or analyze information for or otherwise contribute in any way in preparing or verifying these reports should strive to ensure that the Company's financial disclosure is accurate and transparent and that the Company's reports contain all of the information about the Company that would be important to enable stockholders and potential investors to assess the soundness and risks of the Company's business and finances and the quality and integrity of the Company's accounting and disclosures. Such employees must cooperate fully with the

Company's accounting and internal audit departments, as well as the Company's independent public accountants and counsel. Each person must promptly report (in accordance with the Company's Whistleblower Policy) any information he or she may have concerning (a) significant deficiencies in the design or operation of internal and/or disclosure controls that could adversely affect the Company's ability to record, process, summarize and report financial data or (b) any fraud that involves management or other employees who have a significant role in the Company's financial reporting, disclosures or internal controls.

In addition to the foregoing, the Chief Executive Officer and Chief Financial Officer of the Company and each subsidiary of the Company (or persons performing similar functions), and each other person that is involved in the financial reporting of the Company, must familiarize himself or herself with the disclosure requirements applicable to the Company as well as the business and financial operations of the Company. Accordingly, it is the responsibility of such individuals to promptly bring to the attention of the Audit Committee any untrue statement of a material fact and any omission of a material fact of which he or she may become aware pertaining to information that (a) affects the disclosures made by the Company in its public filings or (b) must otherwise be disclosed pursuant to the Company's policies and procedures regarding accounting standards and documentation.

In addition:

- no employee may take or authorize any action that would cause the Company's financial records or financial disclosure to fail to comply with generally accepted accounting principles, the rules and regulations of the SEC or other applicable laws, rules and regulations;
- all employees must cooperate fully with the Company's accounting personnel, as well as the Company's independent public accountants and counsel, respond to their questions with candor and provide them with complete and accurate information to help ensure that the Company's books and records, as well as the Company's reports filed with the SEC, are accurate and complete; and
- no employee should knowingly make (or cause or encourage any other person to make) any false or misleading statement in any of the Company's reports filed with the SEC or knowingly omit (or cause or encourage any other person to omit) any information necessary to make the disclosure in any of the Company's reports accurate in all material respects.

Any employee who becomes aware of any departure from these standards has a responsibility to report his or her knowledge promptly to their Subsidiary CEO, the Chief Operating Officer, the Board, one of the other compliance resources described in Section 18 below, or in accordance with the provisions of the Company's Whistleblower Policy. The Whistleblower Policy is a supplement to the Code and should be read in conjunction with the Code.

10. Fair Dealing

The Company strives to outperform its competition fairly and honestly. Advantages over the Company's competitors are not to be obtained through unethical or illegal business practices. Acquiring proprietary information from others through improper means, possessing trade secret

information that was improperly obtained, or inducing improper disclosure of confidential information from past or present employees of other companies is prohibited, even if motivated by an intention to advance the Company's interests. If information is obtained by mistake that may constitute a trade secret or other confidential information of another business, or if you have any questions about the legality of proposed information gathering, you must consult your Subsidiary CEO or the Chief Operating Officer, as further described in Section 18 below.

You are expected to deal fairly with the Company's customers, suppliers, employees and anyone else with whom you have contact in the course of performing your job. Be aware that the Federal Trade Commission Act provides that "unfair methods of competition in commerce, and unfair or deceptive acts or practices in commerce, are declared unlawful." It is a violation of the Federal Trade Commission Act to engage in deceptive, unfair or unethical practices, and to make misrepresentations in connection with sales activities.

Employees involved in procurement have a special responsibility to adhere to principles of fair competition in the purchase of products and services by selecting suppliers based exclusively on normal commercial considerations, such as quality, cost, availability, service and reputation, and not on the receipt of special favors.

11. Anti-Bribery and Foreign Corrupt Practices Act

The United States (through the Foreign Corrupt Practices Act ("*FCPA*")) and many foreign governments, through their respective anti-bribery laws, make it illegal to offer or provide, directly or through a third party, anything of value to a foreign government official in order to influence an act, or decision to obtain, retain and/or direct business or to secure an improper advantage of any kind.

The Company strictly prohibits all directors and employees from giving, offering, promising or paying anything of value to government officials directly or indirectly with the purpose of obtaining or retaining business or otherwise securing an improper advantage. All directors and employees must take reasonable steps to ensure that business partners and other third parties understand that the Company expects them to act with the same level of honesty and integrity in any activity engaged in for or on behalf of the Company.

The FCPA contains an exception for "facilitation payments", which are small amounts paid to secure the performance of routine government actions. No facilitation payments may be made by anyone in the Company without prior written approval from the Chief Operating Officer.

The Company may also be responsible for the actions of those acting on our behalf. It is therefore important to select those persons and entities carefully and to ensure that they are properly monitored while doing business for us.

12. Gifts and Entertainment

Business gifts and entertainment are meant to create goodwill and sound working relationships and not to gain improper advantage with customers or facilitate approvals from government officials. The exchange, as a normal business courtesy, of meals or reasonable entertainment is a common and acceptable practice as long as it is not extravagant. Unless express

permission is received from your Subsidiary CEO, the Chief Operating Officer or the Board, gifts and entertainment cannot be offered, provided or accepted by any employee unless consistent with customary business practices and not excessive in value. This principle applies to Company's transactions everywhere in the world, even where the practice is widely considered "a way of doing business." Employees should not accept gifts or entertainment that may reasonably be deemed to affect their judgment or actions in the performance of their duties. The Company's customers, suppliers and the public at large should know that the Company's employees' judgment is not for sale.

Under some state and federal statutes, such as the FCPA, giving anything of value to a government official to obtain or retain business or favorable treatment is a criminal act subject to prosecution and conviction. Discuss with your Subsidiary CEO or the Chief Operating Officer any proposed entertainment or gifts if you are uncertain about their appropriateness.

13. Electronic Communications and Internet Use

The use of the Company's electronic systems, including computers, and all forms of Internet/intranet access, is for company business and for authorized purposes only. Brief and occasional personal use of the electronic mail system or the Internet is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense or harm to the Company or otherwise violate this Code. Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities. Electronic communication should not be used to solicit or sell products or services that are unrelated to the Company's business; distract, intimidate, or harass coworkers or third parties; or disrupt the workplace.

The following guidelines have been established for using the Internet, Company-provided cell phones and e-mail in an appropriate, ethical, and professional manner:

- Internet, company-provided equipment (*e.g.*, cell phone, laptops and computers), and services may not be used for transmitting, retrieving, or storing any communications of a defamatory, discriminatory, harassing or pornographic nature.
- The following actions are not tolerated: using disparaging, abusive, profane or offensive language; creating, viewing or displaying materials that might adversely or negatively reflect upon the Company or be contrary to the Company's best interests; and engaging in any illegal activities, including piracy, cracking, extortion, blackmail, copyright infringement, and unauthorized access of any computers and company-provided equipment such as cell phones and laptops.
- Employees may not copy, retrieve, modify or forward copyrighted materials, except with permission or as a single copy to reference only.
- Employees must not use the system in a way that disrupts its use by others. Employees must not send or receive large files that could be saved/transferred via thumb drives. Employees are prohibited from sending or receiving files that are not related to work.

- Employees should not open suspicious e-mails, pop-ups or downloads. Due to risk of viruses and malware, Employees should not download attachments from unrecognized sources.
- Employees must be aware that the electronic mail messages sent and received using Company equipment or Company-provided Internet access, including web-based messaging systems used with such systems or access, are **not private** and are subject to viewing, downloading, inspection, release, and archiving by Company officials at all times.
- No employee may access another employee's computer, computer files, or electronic mail messages without prior authorization from either the employee or an appropriate Company official.
- The Company prohibits the use in the workplace of any type of camera phone, cell phone camera, digital camera, video camera, or other form of recording device to record the image or other personal information of another person, if such use would constitute a violation of a civil or criminal statute that protects the person's right to be free from harassment or from invasion of the person's right to privacy. Employees may take pictures and make recordings during non-working time in a way that does not violate such civil or criminal statutes. Any suspected incident of fraud or theft should be reported for investigation immediately. The Company reserves the right to report any illegal use of such devices to appropriate law enforcement authorities.

Privacy Expectations & Right to Monitor

The Company owns the rights to all data and files in any computer, network, or other information system used in the Company and to all data and files sent or received using any company system or using the Company's access to any computer network, to the extent that such rights are not superseded by applicable laws relating to intellectual property. Employees should **not** expect privacy in any information or activity conducted, sent, performed, or viewed on or with Company equipment or Internet access. Employees should assume that whatever they do, type, enter, send, receive, and view on Company electronic information systems is electronically stored and subject to inspection, monitoring, evaluation, and Company use at any time

The Company reserves the right to monitor electronic mail messages (including personal/private/instant messaging systems) and their content, as well as any and all use by employees of the Internet and of computer equipment used to create, view, or access e-mail and Internet content. The Company has the right to inspect any and all files stored in private areas of the network or on individual computers or storage media in order to assure compliance with Company policies and state and federal laws. The Company routinely monitors use of company supplied technology. Inappropriate or illegal use or communications may be subject to disciplinary action up to and including termination of employment.

Social Media—Acceptable Use

Use of social media (*e.g.*, Facebook, Twitter, LinkedIn) is a common way of communicating and doing business. Below are guidelines for social media use:

- Employees may not post financial, confidential, sensitive, or proprietary information about the Company, employees or applicants.
- Employees may not post obscenities, slurs or personal attacks that can damage the reputation of the Company, employees, or applicants.
- U.S. federal law has strict requirements concerning testimonials and endorsements. When posting on social media sites concerning Company-related matters, employees must identify themselves as a Company employee and use the following disclaimer: *“The opinions expressed on this site are my own and do not necessarily represent the views of GTY Technology Holdings Inc.”* Any such opinions must be accurate and truthful.
- The Company may monitor content posted on the Internet. Policy violations may result in discipline up to and including termination of employment.

Solicitations, Distributions and Posting of Materials

The Company prohibits the solicitation, distribution, and posting of materials on or at Company property by any employee or nonemployee, except as may be permitted by this Code. The sole exceptions to this Code are charitable and community activities supported by Company management and Company-sponsored programs related to the Company’s products and services.

14. Protection and Proper Use of Company Assets

All employees are expected to protect the Company’s assets and ensure their efficient use. Theft, carelessness and waste have a direct impact on the Company’s financial condition and results of operations. The Company’s property, such as office supplies, computer equipment, laboratory supplies and office, manufacturing or laboratory space, is expected to be used only for legitimate business purposes, although incidental personal use may be permitted. You may not, however, use the Company’s corporate name, any brand name or trademark owned or associated with the Company or any letterhead stationery for any personal purpose. The obligation to protect the Company’s assets includes the Company’s proprietary information. Proprietary information includes intellectual property such as trade secrets, patents, trademarks, and copyrights, as well as business and marketing plans, engineering and manufacturing ideas, designs, databases, records and any non-public financial data or reports. Unauthorized use or distribution of this information is prohibited and could also be illegal and result in civil or criminal penalties.

You may not, while acting on behalf of the Company or while using its computing or communications equipment or facilities, either:

- access the internal computer system (also known as “hacking”) or other resource of another entity without express written authorization from the entity responsible for operating that resource; or

- commit any unlawful or illegal act, including harassment, libel, fraud, sending of unsolicited bulk email (also known as “spam”) in violation of applicable law, trafficking in contraband of any kind, or espionage.

If you receive authorization to access another entity’s internal computer system or other resource, you must make a permanent record of that authorization so that it may be retrieved for future reference, and you may not exceed the scope of that authorization.

Unsolicited bulk email is regulated by law in a number of jurisdictions. If you intend to send unsolicited bulk email to persons outside of the Company, either while acting on the Company’s behalf or using the Company’s computing or communications equipment or facilities, you should contact your Subsidiary CEO or the Chief Operating Officer for approval.

All data residing on or transmitted through the Company’s computing and communications facilities, including email and word processing documents, is the property of the Company and subject to inspection, retention and review by the Company, with or without an employee’s or third party’s knowledge, consent or approval, in accordance with applicable law. Any misuse or suspected misuse of the Company’s assets must be immediately reported to your Subsidiary CEO or the Chief Operating Officer.

15. Confidentiality

One of the Company’s most important assets is its confidential information. As an employee of the Company, you may learn of information about the Company that is confidential and proprietary. You also may learn of information before that information is released to the general public. Employees who have received or have access to confidential information should take care to keep this information confidential. Confidential information includes non-public information that might be of use to competitors or harmful to Company or its customers if disclosed, such as business and marketing plans, financial information, scientific data, engineering and manufacturing ideas, designs, databases, customer lists, pricing strategies, personnel data, personally identifiable information pertaining to the Company’s employees, customers or other individuals (including, for example, names, addresses, telephone numbers and social security numbers), and similar types of information provided to the Company by its customers, suppliers and partners. This information may be protected by patent, trademark, copyright and trade secret laws.

In addition, because the Company interacts with other companies and organizations, there may be times when you learn confidential information about other companies before that information has been made available to the public. You must treat this information in the same manner as you are required to treat the Company’s confidential and proprietary information. There may even be times when you must treat as confidential the fact that the Company has an interest in, or is involved with, another company.

You are expected to keep confidential and proprietary information confidential unless and until that information is released to the public through approved channels (usually through a press release, a filing with the SEC or a formal communication from a member of senior management, as further described in Section 18 below). Every employee has a duty to refrain from disclosing to any person confidential or proprietary information about the Company or any other company learned in the course of employment with the Company, until that information is disclosed to the

public through approved channels. This policy requires you to refrain from discussing confidential or proprietary information with outsiders and even with other employees of the Company, unless those fellow employees have a legitimate need to know the information in order to perform their job duties. Unauthorized use or distribution of this information could also be illegal and result in civil liability and/or criminal penalties.

You should also take care not to inadvertently disclose confidential information. Materials that contain confidential information, such as memos, notebooks, data storage devices and laptop computers, should be stored securely. Unauthorized posting or discussion of any information concerning the Company's business, information or prospects on the Internet is prohibited. You may not discuss the Company's business, information or prospects in any "chat room," regardless of whether you use your own name or a pseudonym. Be cautious when discussing sensitive information in public places like elevators, airports, restaurants and "quasi-public" areas within the Company, such as the reception area. All Company e-mails, voicemails and other communications are presumed confidential and should not be forwarded or otherwise disseminated outside of the Company, except where required for legitimate business purposes.

In addition to the above responsibilities, if you are handling information protected by any privacy policy published by the Company, then you must handle that information in accordance with the applicable policy.

16. Media/Public Discussions

It is the Company's policy to disclose material information concerning the Company to the public only through specific limited channels to avoid inappropriate publicity and to ensure that all those with an interest in the company will have equal access to information. All inquiries or calls from the press should be referred to the Chief Executive Officer or Chief Financial Officer. The Company has designated its Chief Executive Officer and Chief Financial Officer as the company's official spokespersons for financial matters and for marketing, technical and other related information. Unless a specific exception has been made by the Chief Executive Officer or the Chief Financial Officer, these designees are the only people who may communicate with the press on behalf of the Company. You also may not provide any information to the media about the Company off the record, for background, confidentially or secretly.

17. Waivers

Waivers of the Code may only be granted by the Chief Operating Officer; provided, however, that any waiver of the Code for executive officers (including, where required by applicable laws, the Company's principal executive officer, principal financial officer, principal accounting officer or controller (or persons performing similar functions)) or members of the Board may be granted only by the Board or a committee of the Board. Any such waiver of the Code for executive officers or members of the Board, and the reasons for such waiver, will be disclosed as required by applicable laws, rules or securities market regulations.

18. Compliance Standards and Procedures

Compliance Resources

The Company's Chief Operating Officer oversees compliance with the Code and is the person to whom you can address any questions or concerns.

In addition to fielding questions or concerns with respect to potential violations of this Code, the Chief Operating Officer is responsible for:

- investigating possible violations of the Code;
- distributing copies of the Code annually via e-mail to each employee with a reminder that each employee is responsible for reading, understanding and complying with the Code;
- updating the Code as needed and alerting employees to any updates, with appropriate approval of the Board, to reflect changes in the law, the Company's operations and in recognized best practices, and to reflect the Company's experience; and
- otherwise promoting an atmosphere of responsible and ethical conduct.

Your most immediate resource for any matter related to the Code is your Subsidiary CEO. He or she may have the information you need or may be able to refer the question to another appropriate source. There may, however, be times when you prefer not to go to your Subsidiary CEO. In these instances, you should feel free to discuss your concern with the Chief Operating Officer. If you are uncomfortable speaking with the Chief Operating Officer, please contact the Chairman of the Corporate Governance and Nominating Committee. If your concern involves potential misconduct by another person and relates to questionable accounting or auditing matters under the Whistleblower Policy, you may report that violation in accordance with the procedures set forth in such policy.

Clarifying Questions and Concerns; Reporting Possible Violations

If you encounter a situation or are considering a course of action and its appropriateness is unclear, discuss the matter promptly with your Subsidiary CEO or the Chief Operating Officer; even the appearance of impropriety can be very damaging and should be avoided.

If you are aware of a suspected or actual violation of Code standards by others, you have a responsibility to report it. You are expected to promptly provide a compliance resource with a specific description of the violation that you believe has occurred, including any information you have about the persons involved and the time of the violation. Whether you choose to speak with your Subsidiary CEO or to the Chief Operating Officer, you should do so without fear of any form of retaliation. The Company will take prompt disciplinary action against any employee who retaliates against you, up to and including termination of their employment.

Subsidiary CEOs must promptly report any complaints or observations of Code violations to the Chief Operating Officer. If you believe your Subsidiary CEO has not taken appropriate action, you should contact the Chief Operating Officer directly. The Chief Operating Officer will investigate all reported possible Code violations promptly and with the highest degree of confidentiality that is possible under the specific circumstances. All directors, officers and employees are expected to cooperate in any internal investigation of misconduct. Neither you nor

your Subsidiary CEO may conduct any preliminary investigation, unless authorized to do so by the Chief Operating Officer. Your cooperation in the investigation will be expected. As needed, the Chief Operating Officer will consult with the Human Resources Department and/or the Board. It is the Company's policy to employ a fair process by which to determine violations of the Code.

With respect to any complaints or observations of Code violations that may involve accounting, internal accounting controls and auditing concerns, the Chief Operating Officer shall promptly inform the Board, and such other persons as the Board determines to be appropriate under the circumstances shall be responsible for supervising and overseeing the inquiry and any investigation that is undertaken.

If any investigation indicates that a violation of the Code has probably occurred, the Company will take such action as it believes to be appropriate under the circumstances. If the Company determines that an employee is responsible for a Code violation, he or she will be subject to disciplinary action up to, and including, termination of employment and, in appropriate cases, civil legal action or referral for regulatory or criminal prosecution. Appropriate action may also be taken to deter any future Code violations.

19. Dissemination and Amendment

This Code will be distributed to each new employee, officer and director of the Company upon commencement of his or her employment or other relationship with Company and will also be distributed annually. The Company may amend this Code. The Company will disclose any amendments pertaining to executive officers or directors as required by law or securities market regulations. The most current version of this Code can be found on Company's website.

20. Certification

You should read this Code carefully. Promptly certify your understanding of, and intent to comply with, this policy by signing the certification attached hereto.

GTY Technology Holdings Inc.

Code of Business Conduct and Ethics

Certification as applicable to my work responsibilities:

1. I will deal honestly and ethically with the Company and on the Company’s behalf in all matters.
2. I will avoid actual or apparent conflicts with the Company’s interests.
3. I will advance the Company’s business interests when the opportunity to do so arises.
4. I will comply with the Company’s standards, policies and procedures regarding gifts, meals and entertainment.
5. I will ensure the accuracy and integrity of the Company’s books, records and accounts.
6. I will protect the confidential information of customers and others which I receive in the course of conducting Company business.
7. I will ensure that, in all reports and documents filed with or submitted to the United States Securities and Exchange Commission by the Company and in other public communications made by the Company, to the extent I am involved with the preparation thereof, the Company’s disclosures are full, fair, accurate, timely and understandable.
8. I will comply with all laws, rules and regulations applicable to my work responsibilities in every country in which the Company does business.
9. I will comply with all Company standards, policies and procedures.
10. I will protect the Company’s assets and promote their efficient and legitimate business use.
11. I will protect the Company’s confidential information.
12. I will protect the health and safety of the Company employees.
13. I will use the Company’s electronic media for legitimate business purposes.

I certify that I have received, read, understood and will abide by the **Code of Business Conduct and Ethics**.

_____ Signature

_____ Name

_____ Subsidiary Company

_____ Date

Version 1: July 1, 2019
Version 2: July 1, 2020