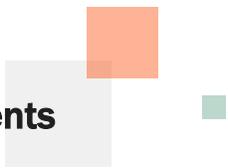


# Code of Conduct and Ethics



## Table of Contents

### 1. Introduction

### 2. Culture & Values

Our Culture and values serve as the foundation for our policies, procedures, and expectations.

### 3. Your Personal Responsibilities

Each employee is responsible for acting ethically, consistent with this Code and the Company's values and policies, as well as all applicable laws.

### 4. Reporting Concerns

Employees should immediately report any suspicions or awareness of dishonest or unethical behavior, including violations of this Code, the Company's policies or any applicable laws. The Company has several ways for you to report your concerns, including on an anonymous basis and without fear of retaliation.

### 5. Respectful and Safe Work Environment

We all are responsible to create and maintain a work environment that is safe and drug free and free of sexual or other workplace harassment, discrimination, or violence.

### 6. The Law and Business Ethics

You should not engage in any activity that is inconsistent with the Company's interests actual or perceived, or results in you receiving a benefit exceeding a nominal amount.

### 7. Responsibility to our Stockholders

Protect the Company's brand, reputation, assets, and intellectual property. Maintain accurate business records and retain records in compliance with Company policies and applicable laws. Responsibly use available resources such as e-mails, telephones, and Internet access.

### 8. Administration of this Code

The Company administers this Code and you shall certify your agreement with and understanding of this Code as requested by the Company.

## 1. Introduction

The Sterling Code of Conduct and Ethics (this “Code”) embodies our commitment to the highest standards of ethical behavior and legal compliance. Strict adherence to this Code will protect the reputation of the Company and promote a workplace characterized by dignity and respect for individuals.

We are driven by a passion to keep the workplace safe and operating in an ethical manner, while protecting the rights of both businesses and individuals. Protecting the safety and reputation of our clients, their employees and customers, and protecting the integrity and confidentiality of the personal information in our care is at the heart of Sterling.

This Code, which has been approved by the Company’s leadership and the Audit Committee of its Board of Directors (the “Audit Committee”), requires that all employees adhere to a set of Company values, principles, and behaviors. While this Code attempts to address the most common legal and ethical situations that we may encounter, it cannot address every situation or issue that may arise. If you encounter an issue that you feel is not addressed in this Code, please seek guidance from your manager, People & Culture representative, Counsel of Corporate Ethics and Compliance or the Chief Legal and Risk Officer of the Company.

This Code applies to:

- All employees of, regardless of location; Sterling Check Corp. and each of its subsidiaries (collectively, “Sterling”, the “Company”, “we” or “our”) and
- Members of the Board of Directors when they act in their capacity as directors of the Company.

This Code does not apply to any entity where the Company has neither legal nor operational control (e.g. minority investments).

None of our personnel documents and benefit plans, including this Code, constitute, or is intended to constitute, an express or implied contract guaranteeing continued employment for an employee. Nothing in this Code or in any other

document or policy is intended to violate any local, state or federal law. This Code shall be the Company’s “code of ethics” within the meaning of Section 406 of the Sarbanes-Oxley Act of 2002 and the rules promulgated thereunder.

All employees are expected to conduct themselves in line with our Company values and to avoid any situations in which there may be even an appearance of improper conduct. Employees are required to comply with the rules and regulations of all U.S. and non-U.S. governmental entities and other private and public regulatory agencies to which the Company is subject, including any exchanges on which the Company’s securities may be listed. Employees are expected to understand and comply with laws, rules and regulations applicable to their jobs or positions and to know when to seek advice from their manager, People & Culture representative, Counsel of Corporate Ethics and Compliance or the Chief Legal and Risk Officer of the Company.

## 2. Culture & Values

### It’s all about people

Our business is about helping people find the right people. We care deeply about colleagues, clients and their candidates.

### The client is always in the room

We exist to help our clients build a foundation of trust and safety. We make decisions that are best for the client, based on data and judgment, not ego and politics.

### Deliver results: They matter

We play to win. We are smart, fast and driven. We take risks, make mistakes and learn from them. We deliver.

### Start with trust and prove it everyday

We trust each other and prove ourselves worthy of trust to our clients and colleagues every day.

### 3. Your Personal Responsibilities

As an integral member of the Sterling team, it is your responsibility to act ethically and responsibly.

You should represent yourself, your manager, your department, and the Company in a way that is consistent with our values, this Code, our policies, and the law.

For our managers, it is imperative that you set the example for members of your team. We must have an environment that is open and respectful, where we constructively challenge each other to make the Company better each and every day.

As a tech-enabled services company operating in a regulated environment, following the law is the foundation of our operations. All employees must act in accordance with all applicable laws.

As an employee, you are expected to follow this Code along with all Company policies and procedures and applicable laws at all times. Any violation of this Code and/or policies and procedures is subject to disciplinary action up to and including termination. In the case that a law has been violated, civil and/or criminal penalties may also be imposed by a government agency or a court of law. If you believe a local law or policy is in conflict with this Code, you should consult with a People & Culture representative, the Counsel for Corporate Ethics and Compliance or the Chief Legal and Risk Officer of the Company. You may also contact our Ethics Hotline—See Section 4 of this Code.

### 4. Reporting Concerns

If you are aware of or suspect any dishonest or unethical behavior including but not limited to violations of this Code, policies and procedures, and/or applicable laws, you have a duty to report the issue immediately to your manager, People & Culture representative, the Counsel for Corporate Ethics and Compliance, the Chair of the Audit Committee, the head of internal audit, the Chief Legal and Risk Officer of the Company, or the Ethics Hotline. A failure to report may result in disciplinary action.

Conduct that must be reported includes, but is not limited to:

- Dishonesty or questionable practices in accounting, internal accounting controls or auditing matters, including, but not limited to:
  - Fraud or deliberate error in the preparation, maintenance, evaluation, review or audit of financial statements of the Company;
  - Fraud or deliberate error in the recording and maintaining of the Company's financial records;
  - Deficiencies in, or non-compliance with, the Company's internal controls over financial reporting;
  - Misrepresentation or false statements regarding a matter contained in the Company's financial records, financial statements, audit reports or any filings made with the Securities and Exchange Commission (including periodic or current reports);
  - Deviation from full and fair reporting of the Company's financial condition and results;
  - Substantial variation in the Company's financial reporting methodology from prior practice or from generally accepted accounting principles without adequate public disclosure;
  - Issues affecting the independence of the Company's independent registered public accounting firm;
  - Falsification, concealment or inappropriate destruction of corporate or financial records; or
  - Theft, fraud or other misappropriation of Company assets;

- Possible non-compliance with applicable legal and regulatory requirements or this Code; and
- Alleged retaliation against employees and other persons who make, in good faith, accounting allegations or compliance allegations.

The Company will immediately investigate any reported matter related to dishonest or unethical behavior, including but not limited to violations of this Code, Company policies and procedures, and/or applicable laws. The Company will make every attempt to protect confidentiality during and after any investigation.

Similarly, if you are a manager and you have received information from an employee concerning activity that may violate this Code, Company policies and procedures, and/or applicable laws, you have a duty to report the issue immediately to your manager (unless the conduct of your manager is at issue, in which case, to the Chief Legal and Risk Officer of the Company).

The investigation may include but not be limited to the following:

- An objective gathering of the facts.
- Interviews of employees or others who may have knowledge of the incident reported.
- Recommendation of corrective or disciplinary action as the Company determines appropriate.

## Anti-Retaliation

If you report any dishonest or unethical behavior including but not limited to violations of this Code, Company policies and procedures, and applicable laws in good faith, you can do so without fear of any retaliation or punishment. None of the Company, the Audit Committee or any director, officer, employee, contractor, subcontractor or agent of the Company will discharge, demote, suspend, threaten, harass or in any other manner discriminate or retaliate, directly or indirectly, against any person who

- In good faith reports what they believe is a violation of this Code, our policies or the law.
- In good faith raises a compliance question or asks for advice regarding a business decision, practice, or action.
- Cooperates or participates in an investigation.

No action will be taken against any party who submits a report in good faith, even if the facts alleged are not confirmed by subsequent investigation. However, if, after investigation, a report is found to be without substance and to have been made for malicious or frivolous reasons, any employee who made the report could be subject to disciplinary action, up to, and including, termination of employment.

Unless necessary to conduct an adequate investigation or compelled by judicial or other legal process, neither the Company, the Audit Committee nor any director, officer or employee of the Company shall (i) reveal the identity of any person who makes a report and asks that such person's identity remain confidential, or (ii) make any effort, or tolerate any effort made by any other person or group, to ascertain the identity of any person who makes a report anonymously.

## How Do I Report an Issue?

There are several different ways to report any dishonest or unethical behavior including but not limited to violation of this Code, Company policies and procedures, and applicable laws or ask related questions.

You can reach out directly to your manager, People & Culture representative, the Chair of the Audit Committee, the head of internal audit, the Counsel for Corporate Ethics and Compliance or the Chief Legal and Risk Officer of the Company.

You may also contact our Ethics Hotline. If you choose to contact the Ethics Hotline, you have the option to remain anonymous. However, please be aware that anonymity may limit the Company's ability to investigate your concerns.

The Ethics Hotline telephone number is:

- **Toll Free (US & Canada only):**  
877-774-7710
- **International (Toll):**  
1-651-602-2391  
(The “1” is the country code for US)

You can also contact the Ethics Hotline by:

- **Email:** [reports@lighthouse-services.com](mailto:reports@lighthouse-services.com)  
(must reference Sterling in the subject line of email report)
- **Website:** [www.lighthouse-services.com/sterlingcheck](http://www.lighthouse-services.com/sterlingcheck)
- **SterLINK:** Ethics Hotline information is available on SterLINK by clicking the provided link.

## 5. Respectful and Safe Work Environment

The Company is committed to creating and maintaining a work environment where everyone can work, learn, and recommend ideas in a climate of mutual respect that is free of harassment and discrimination. Creating a positive and diverse work culture is the responsibility of every employee.

### Anti-Harassment

Sexual harassment and other work place harassment will not be tolerated. See the Company’s Anti-Harassment Policy for further details.

### Anti-Violence

It is the Company’s intent to promote a safe work environment. You are prohibited from any acts that may make an individual feel threatened physically or verbally or intimidated in any manner. No act of violence, expression of hostility or intimidation of others will be tolerated.

The Company also prohibits the possession of weapons in the work place. This includes any part of the workplace facility, parking lots and at work related functions, unless otherwise provided by applicable law.

### Anti-Drug

You are not permitted to work under the influence of illegal drugs or alcohol, as this may create an unsafe work environment and impair the quality and standard of work.

### Behavior Outside of Work

It is imperative that your behavior outside of work remains within the law. Negative information on a background check that relates to an employee’s ability to perform their job in a manner consistent with this Code, could result in disciplinary action up to and including termination. The Company conducts a pre-employment background check on all employees and may conduct post-employment background checks at such times that it determines.

## 6. The Law and Business Ethics

You are an ambassador of the Company and are expected to conduct yourself with the highest ethical standards. You are expected to adhere to this Code, our values and our policies and all applicable law in all business dealings. Always remember that your individual conduct projects an image of the entire organization.

Your business dealings must never be influenced by any level of corruption. Corruption is an action to obtain any advantage or benefit (for the Company, yourself, or anyone else) through improper or illegal means. Corrupt activities may not only be a violation of this Code or Company policy; they may also be a violation of the law. Any violation of applicable laws may result in criminal and civil penalties. You should immediately report any suspicion or awareness of an unethical, improper, or illegal activity to your manager, People & Culture representative, the Counsel for Corporate Ethics and Compliance, the Chair of the Audit Committee, the head of internal audit, the Chief Legal and Risk Officer of the Company or the Ethics Hotline. If you have any questions of whether an action is unethical, improper, or illegal, you should inquire of the resources noted above for clarification.

## THE LAW

### Anti-Bribery

Bribery is the act of giving money, a gift, or any other thing of value (e.g., travel and entertainment, business opportunities, employment) to a government official or private person to alter the behavior of the recipient. Engaging in bribery is a violation of this Code. You should never, directly or indirectly through a third-party, offer any form of money or gift to anyone (government official or private person) to influence a business decision. A “government official” is anyone who works for, or is an agent of, a government-related entity (including businesses and institutions that are owned or controlled by government entities). This includes entities at the local, state, and federal levels, U.S. and foreign. A “government official” also includes candidates for political office, officials of political parties, and employees of international organizations (e.g., United Nations, World Bank). When in doubt, treat a third party as a “government official” for purposes of this Code of Conduct.

\*Note that paying an individual courthouse employee or other custodian of records for public or private record data without the express permission of the court or other institution could be an example of bribery.

The US Foreign Corrupt Practices Act (FCPA) makes bribery of foreign government officials a crime and applies everywhere around the world where the Company conducts business. Any payments or gifts to a government official must be pre-approved (in writing) by the Chief Legal and Risk Officer of the Company. The FCPA also requires public companies to make and keep accurate books and records and to devise and maintain an adequate system of internal accounting controls.

The UK Bribery Act makes it a crime to offer to pay a bribe to any foreign public official or private person. In addition, the failure to prevent a bribe is also considered a crime under the UK Bribery Act.

Other nations may have similar laws not listed here, and the Company’s anti-bribery policy extends to require compliance with all applicable

laws. The Chief Legal and Risk Officer should be consulted in all cases regarding the potential application of anti-corruption laws to the Company.

### Anti-Kickback

A kickback is a form of compensation or in-kind gift accepted from a vendor, contractor or other commercial entity engaged in business for the purpose of influencing a business decision. Your acceptance of a kickback is strictly prohibited. Similarly, you are prohibited from giving or agreeing to give any kickbacks on behalf of the Company.

The Anti-Kickback Act of 1986 prohibits US federal contractors from accepting any payment or gratuity for the purpose of obtaining a federal contract.

### US Anti-Trust Laws

US anti-trust laws have been enacted to preserve competition among companies engaged with similar business interests. These laws prohibit actions that may restrain trade.

To comply with anti-trust laws, you should avoid the following situations:

- Discussing product pricing with competitors
- Discussing operating costs with competitors
- Discussing marketing information with competitors
- Commenting on a competitor’s product or services in an untruthful or misleading manner.

Should a competitor attempt to discuss pricing, costs, or other financial matter, you should end the conversation and immediately report the incident to the Counsel for Corporate Ethics and Compliance or the Chief Legal and Risk Officer of the Company.

### UK Competition Law

UK Competition Law makes it an offense to enter into agreements or participate in practices, which

have as their object, or effect, the restriction or distortion of competition in the United Kingdom. You have an obligation to comply with UK Competition Law as applicable.

## BUSINESS ETHICS

### Securities Trading Policy

United States securities laws prohibit trading on the basis of material, non-public information (i.e., insider trading). Employees who have access to material non-public information about a company, including Sterling, regardless of its source, are not permitted to use or share that information for their personal benefit for securities trading purposes. All non-public information about Sterling, its customers or other business parties should be considered confidential information. Trading in securities of Sterling or other public companies while in possession of material, non-public information may constitute illegal insider trading, and it is also may be illegal to communicate or “tip” such information to others who do not have a legitimate business need for acquiring the information.

See the Company’s Securities Trading Policy for further details.

### Conflicts of Interest

As reviewed in our Employee Handbook, employees and their immediate families must avoid having any financial interests that are inconsistent with the best interests of the Company, and must refrain from activities, investments or associations that compete with the Company, interfere with one’s judgment concerning the Company’s best interests, exploit one’s position with the Company for personal gain or might impair, or even appear to impair, their ability to make objective and fair decisions when performing their jobs.

At times, employees may be faced with situations where the business actions they take, on behalf of the Company, may conflict with their own personal or family interests because of the course of action that is best for them personally may not also be the best course of action for the Company.

Examples of potential conflict situations include:

- Having a financial interest in any business transaction with the Company;
- Owning or having a significant financial interest in, or other relationship with, a Company competitor, customer or supplier;
- Competing with the Company while still employed by the Company;
- Diverting business away from the Company while still employed by the Company;
- Using Company assets or labor for personal use;
- Placing Company business with a firm owned or controlled by a Company employee or his or her family;
- Accepting gifts, entertainment or any other benefit of more than a nominal value from a competitor, customer or supplier

Employees are responsible for identifying potential conflicts when they arise, and must notify the Counsel of Corporate Ethics and Compliance or the Chief Legal and Risk Officer of the Company.

### Related Person Transaction

The Company recognizes that transactions with related persons present a heightened risk of conflicts of interests and/or improper valuation or the perception thereof. All such transactions are prohibited without first reporting to, and receiving the written consent of, the Chief Legal and Risk Officer and the Chief Financial Officer of the Company. Further, these transactions will also be reported to the Audit Committee.

A “Transaction with a Related Person” consists of any transaction in which the Company is a participant, and any “Related Person” has a direct or indirect material interest.

Generally, a “Related Person” is any employee or Director of the Company, any nominee for director, any stockholder owning in excess of 5% of the total equity of the Company, and a “Family Member” of any such person.

“Family Member” means any family relationship by blood, marriage or law, and includes a child, stepchild, parent, stepparent, spouse, sibling, mother-in-law, father-in-law, son-in-law, daughter-in-law, brother-in-law, or sister-in-law of a person, and any person (other than a tenant or an employee) sharing the household of such person.

See the Company’s Related Person Transaction Policy for further details.

### Soliciting Donations and Fundraisers

The Company supports and encourages you to participate in charitable causes that positively impact the communities in which we work and live. Participation in any charitable cause is at the sole discretion of an employee. Employees may not make charitable contributions on behalf of the Company without receiving pre-approval (in writing) from the Chief Legal and Risk Officer of the Company.

You may not pressure another employee to support or contribute to any charitable or political cause or use Company resources (including work time and computer resources) to promote such causes. The Company does not make political contributions and does not reimburse employees for political contributions.

### Gifts and Entertainment

Special caution must be exercised when giving or accepting gifts and/or entertainment.

You are prohibited from accepting cash or anything of monetary value except as set forth in this Code. Any accepted gift or entertainment should be limited in value (under \$25 or equivalent local currency) so not to be construed as a “payoff”, “kickback”, bribery or give the appearance of influencing a business decision.

If there is any possibility that an offered gift or entertainment has even the appearance of impropriety, it must not be accepted. In very limited circumstances, if respectfully declining to accept a gift would damage the Company’s goodwill or is otherwise not practicable, the employee should accept the gift but then promptly turn it over to the Chief Legal and Risk Officer of the Company.

Different countries may have social customs and traditions that make it appropriate to accept a gift or entertainment. Some gifts and entertainment may generally be allowed.

Before accepting gifts or entertainment, you should take into account the local custom and laws, and consult with your manager, People & Culture representative, the Counsel of Corporate Ethics and Compliance, or the Chief Legal and Risk Officer of the Company if there is any question as to the propriety.

Accepting gifts and entertainment, as well as multiple gifts or entertainment over a short period of time, may violate Company policy or the law.

- **Acceptable:** You receive a holiday gift basket from a client in appreciation of your efforts such as exemplary service above and beyond client’s expectation.
- **Not Acceptable:** You receive a gift card with monetary value from a client or vendor.

If you are involved in purchasing decisions or have purchasing or vendor management responsibilities, you may not accept any gifts or entertainment from vendors, including but not limited to cash, entertainment travel and gifts.

Just as accepting gifts and entertainment deserves ethical consideration, so too does providing gift and entertainment to clients. Employees providing gifts and entertainment to a client should also observe limits in line with Company expectations. The same Company policy considerations described above for accepting gifts and entertainment apply to conferring gifts and entertainment to clients. No gifts or entertainment shall include cash, an extravagant expense or involve any environment that does not represent the ideals and values of the Company. In addition, no gift or entertainment shall knowingly violate the gift policy of a client.

You should never offer any form of money or gift to a government official to influence a business decision—see Anti-Bribery above.

## Product Quality

The Company is committed to providing our clients with background screening reports that conform to the standards set forth in federal, state, and international law. You have the obligation to perform your respective job responsibilities in accordance with all applicable laws.

## Competitive Intelligence

Gathering information about our competitors plays an important part in the development of our business strategies. Any effort to collect information on a competitor shall be obtained in a legal and ethical manner. In addition to public sources, information may be obtained from customers, consultants, and business partners unless prohibited by confidentiality obligations. We may not accept information about our competitors from sources that we know or have reason to believe is confidential or was otherwise improperly obtained. To the extent we have fellow employees who have previously worked for our competitors we shall not pressure them to share private information about their previous employers. Likewise, it is a violation to share Company related proprietary and confidential information with competitors.

Many countries have anti-competition laws against improperly obtaining competitor information. Under no circumstances shall information be obtained through theft, bribery or any other unethical means.

Should you need guidance regarding the collection of competitor information, please contact the Chief Legal and Risk Officer of the Company.

## Vendor/Suppliers/Contractors/Business Partners

The Company shall have no business relationship with any entity suspected of any illegal or unethical business practices.

If there is any possibility that a vendor or supplier-offered benefit or service has even the appearance of impropriety, it must not be accepted.

## Truth in Marketing

Any advertisement or marketing information that is published must be truthful and not misleading. All marketing claims must be capable of substantiation and such substantiation must be maintained on file by our marketing department.

## Contracts

All contracts including but not limited to those with clients, vendors, agents, third parties, etc. should be in writing and conform to our policies. We must conduct business with our clients, vendors, or any contracting party in accordance with the terms and conditions noted in the contracts.

## External Company Disclosures

The Company is required to comply with the reporting requirements of the Securities and Exchange Commission ("SEC") and the Nasdaq Global Select Market well as applicable provisions of the Sarbanes Oxley Act. The Company must see that all accounting functions operate to the highest standard and that the accounting records maintained are in accordance with those standards as well as local laws and regulations. In addition, the Company is committed to providing full, fair, accurate, timely and understandable disclosure in any reports and documents that it may file with, or submit to the SEC, the Nasdaq Global Select Market and other securities regulators or exchanges, as well as in its other public communications. If you are involved in the preparation of any such Sterling disclosures, or if you provide information as part of the process, you have a responsibility to ensure that disclosures and information are provided in compliance with Sterling's disclosure controls and procedures. Any violation of this policy could lead to disciplinary action up to and including termination. You should promptly bring to the attention of the Counsel of Corporate Ethics and Compliance or the Chief Legal and Risk Officer of the Company any material information of which you may become aware that affects the disclosures made by the Company in its public filings or otherwise.

In connection with its public communications as a public company, Sterling is required to comply with a rule under the United States securities laws referred to as Regulation FD (which stands for “fair disclosure”). Regulation FD mandates that public companies avoid selectively disclosing market-sensitive information to participants in the securities markets.

Accordingly, Sterling employees should not disclose material information about Sterling to reporters or securities market professionals or stockholders that has not been made available to all investors in the Sterling’s securities through the SEC’s EDGAR system and any other means.

Inquiries from reporters or securities market professionals received by any employee or agent of the Company (other than an authorized spokesperson) must be forwarded to the Chief Legal & Risk Officer, the Chief Financial Officer or another authorized spokesperson. Under no circumstances should any attempt be made to handle these inquiries without prior authorization from an authorized spokesperson.

“Securities market professionals” generally include analysts, brokers, dealers, investment companies, hedge funds, institutional investors and investment advisors. Information is “material” if there is a substantial likelihood that an investor would consider the information important in making an investment decision or if the information alters the total mix of information available to the market. Information need not affect the investor’s ultimate investment decision to be material.

A non-exhaustive list of information that could be material includes: Sterling’s earnings forecasts, quarterly or annual results in advance of publishing them on the SEC website or any other means, and significant transactions contemplated by Sterling (for example, acquisitions and dispositions).

Any violation of this policy could lead to disciplinary action up to and including termination.

### **Media and Public Appearance Policy**

Employees are not authorized to comment to the media unless specifically approved to do so by the

Chief Marketing Officer, and may not independently agree to public speaking roles. If you are contacted by the media or event organizers in any way, refer the inquiry to the Marketing Department.

Any violation of this policy could lead to disciplinary action, up to and including termination.

### **Privacy**

Personal information is any information about an identifiable individual, such as name, social security number, data and place of birth, mother’s maiden name, or biometric records. Identity numbers are types of data which are subject to special protections under the law or creates a high risk for individuals if misused, and include Social Security or national identity numbers, driver’s license numbers, passport numbers and dates of birth. Any employee that has access to personal information of other employees, our suppliers, contractors or customers or their applicants and employees or the systems that maintain it, must comply with all applicable policies and laws regarding the collection, use and disclosure of personal information, including any special protections for identity numbers. You should:

- Only access personal information for legitimate business purposes
- Securely store and dispose of personal information
- Transmit personal information only to authorized parties and observe all special rules for transmitting identity numbers
- Immediately report any possible data incidents, including actual or suspected unauthorized access or disclosure of personal information, as well as any violation of privacy or security policies, to the Privacy and Information Security teams

It is the responsibility of every employee to keep all personal information confidential, securely stored (e.g., encrypted and password protected) and ensure secure disposal in accordance with applicable law and Company policy when the

business purpose is completed. Personal information should only be transmitted securely to authorized parties in compliance with Company policy. All materials containing confidential or personal information should be shredded (subject to applicable laws) once they are no longer needed and should never be placed in the ordinary trash receptacles or recycling bins. You are required to report any actual, suspected or potential data incident to the Privacy and Information Security teams as soon as you become aware of it. Information on reporting is available on SterLINK.

See the Company's Privacy Policy for further details.

### **Confidential and Proprietary Information**

Also found in our Employee Handbook, any requests for Confidential Information or Proprietary Information must be pre-approved and coordinated with a People & Culture representative or the Counsel of Corporate Ethics and Compliance. This will ensure Sterling's Confidential Information and Proprietary Information is adequately protected from improper disclosure, and that a prompt response and that accurate, up-to-date materials are supplied to the extent possible without harm to the Company.

The Company's Confidential Information and Proprietary Information is vital to the current operations and future success of the Company. Each employee shall use all reasonable care to protect or otherwise prevent the unauthorized disclosure of such information, including securing documents, limiting access to computers and electronic media, and proper disposal methods, and shall maintain the confidentiality of that information except when disclosure is expressly authorized or is required or permitted by law. If an employee is uncertain whether certain information should be treated as confidential, the employee should presume that such information is confidential and not disclose it without proper authorization.

"Confidential Information" refers to a piece of information, or a compilation of information, in any form (on paper, in an electronic file, or

otherwise), related to the Company's business that the Company has not made public or authorized to be made public, and that is not generally known to the public through proper means.

"Proprietary Information" includes information regarding the Company's business methods, business plans, business contracts, databases, systems, technology, intellectual property, know-how, marketing plans, business development, operations, products, services, research, development, inventions, financial statements, financial projections, financing methods, pricing strategies, customer sources, employee health/medical records, system designs, customer lists, and methods of competing

By way of example, Confidential Information or Proprietary Information includes information regarding the Company's business methods, business plans, business contracts, databases, systems, technology, intellectual property, know-how, marketing plans, business development, operations, products, services, research, development, inventions, financial statements, financial projections, financing methods, pricing strategies, customer sources, employee health/medical records, system designs, customer lists, and methods of competing. Additionally, employees who by virtue of their job responsibilities have the following information, should not disclose such information for any reason, except as required to complete job duties, without the permission of the employee at issue: social security numbers, driver's license or resident identification numbers, financial account, credit or debit card numbers, security and access codes or passwords that would permit access to medical, financial or other legally protected information.

Confidential Information does not include information lawfully acquired by non-management employees about wages, hours or other terms and conditions of employment if used by them for purposes protected under §7 of the National Labor Relations Act.

Nothing in this Code prohibits an employee from communicating with any governmental authority or making a report in good faith and with a

reasonable belief concerning any violations of law or regulations to a governmental authority, or disclosing Confidential Information which the employee acquired through lawful means in the course of his or her employment to a governmental authority in connection with any communication or report, or from filing, testifying or participating in a legal proceeding relating to any violations, including making other disclosures protected or required by any whistleblower law or regulation to the Department of Labor, or any other appropriate government authority. To the extent an employee discloses any Confidential Information in connection with communicating with a governmental authority, the employee will honor the other confidentiality obligations in this Code and will only share such Confidential Information with his or her attorney, or with the government agency or entity. Nothing in this Code shall be construed to permit or condone unlawful conduct, including but not limited to the theft or misappropriation of Company property, trade secrets or information.

When an employee leaves the Company, the employee must return to the Company all of its Confidential Information that the employee has in his/her possession or control, including but not limited to, documents, files, records, manuals, information stored on a computer or on a computer disc, thumb drive, or other peripheral device.

This Confidential Information policy will continue even after the employment relationship ends. If you need clarification regarding this policy please contact your Supervisor or People & Culture Representative.

Employees who violate this policy may be subject to disciplinary action up to and including termination, and may also be subject to civil and/or criminal penalties in accordance with applicable law.

## 7. Responsibility to our Stockholders

We are all ambassadors of the Company and your individual actions can reflect on the entire organization. As such, you are required to always act in the best interest of the Company and our stockholders.

Any misuse of Company resources, or any effort to intentionally conceal, falsify or omit information for your benefit, or the benefit of others, may rise to the level of theft. Such activity may negatively impact stockholder rights. Any violation of this section may result in disciplinary action up to and including termination, or possibly result in the filing of criminal and civil charges.

### Fraud

Fraud can take on different forms, including misrepresentation of facts for personal gain, and misuse of Company resources. Fraud may be a violation of the law, subject to legal action in addition to a violation of this Code. Your actions, or failure to act, are fraudulent when you intentionally conceal, alter, falsify, or omit information for your benefit or the benefit of others. Fraud may be motivated by the opportunity to gain something of value (such as meeting a performance goal or obtaining a payment) or to avoid negative consequences (such as discipline).

Examples of fraud include, but are not limited to:

- Altering numbers to meet productivity goals
- Presenting false medical information to obtain disability benefits
- Falsely reporting time worked to earn more pay or to avoid discipline for being late or absent from work
- Misrepresenting sales or donations of products to obtain unauthorized pricing to customer
- Misstating financial information in our Company's books and records
- Using someone else's credentials

In keeping with the Company's standards of integrity and ethical standards, avoid even the appearance of fraud. For example, spending Company funds without proper approval could create the appearance of fraud, and thus would constitute a violation of this Code. Unless specifically authorized by the Company, employees are never permitted to enter into any agreement on behalf of the Company.

## Accurate Business Records

Company business records (including any document or communication in paper or electronic form that is maintained in the course of business) must always be accurate. Whether it is a financial statement, expense report, time card, sales commission, presentation, business contract or government reports, all documents must be truthful and completed with the highest level of integrity. Any effort to falsify, omit, misstate, alter, or conceal information of any business record will be a clear violation of this Code and you will be subject to disciplinary action.

You are accountable for the accuracy of the business records that you handle in the normal course of business. You should never:

- Falsify, omit, misstate, alter or conceal any information or otherwise misrepresent the facts on a Company record
- Encourage or allow anyone else to compromise the accuracy and integrity of our records

If you notice an inaccuracy in a Company record, or a failure to follow our internal control processes, you must promptly report it to your manager, People & Culture representative, the Counsel of Corporate Ethics and Compliance, the Chair of the Audit Committee, the head of internal audit, the Chief Legal and Risk Officer of the Company or the Ethics Hotline.

All financial reporting must comply with the applicable laws, rules, and regulations that govern financial accounting and reporting. All financial entries are to be in compliance with Generally Accepted Accounting Principles (GAAP).

## Records Management

You should maintain business records in accordance with all applicable laws and regulations for all documents, files, electronic records, and emails.

A company our size generates a large volume of records and documents each day. The business records that you work with must be maintained, retained, and destroyed in accordance with all

applicable legal and regulatory recordkeeping requirements.

You should consult the Legal Department if you have specific questions about the retention period of a document, or if you have questions, concerning the documents referred to in a legal hold notification. Destruction of documents subject to a legal hold notice, even inadvertently, could expose the Company and you to civil and criminal liability.

## Protection of Company Assets

You are required to protect Company assets and ensure their efficient use. Carelessness and waste have a direct impact on the Company's efficiency and profitability. All Company assets should only be used for legitimate business purposes.

If your position includes purchasing authority or otherwise entering contractual commitments, you are expected to negotiate for terms in the best interest of the Company. All purchases and contracts must have the appropriate approvals including legal review, in accordance with the Company's Schedule of Authority regarding contractual commitments, before any purchasing transaction or other contract is completed.

Your scheduled work hours are considered a Company asset. Do not engage in personal activities at work as they may interfere with your ability to fulfill your work responsibilities. This includes the inappropriate use of Company equipment such as your computer, telephone, and photocopiers (incidental use in accordance with this Code is permitted). Equipment is provided for your business needs only.

## Audits and Investigations

At times, you may have a duty to preserve information relevant to that matter, which may include, but is not limited to, e-mails, reports, documentation, and electronic and paper files. You may also be asked to gather data or information related to the audit, investigation or other legal matter in which you are asked to participate. Your timely compliance with data and information requests is mandatory.

## Intellectual Property

The Company's intellectual property is an invaluable asset that must be protected at all times. Intellectual property includes, but is not limited to, our strategic plans, name, trademarks, logo, copyrights, patents, operational process, data sources, trade secrets, innovations, reputation, software, technology, and any information and data for which the Company considers proprietary information. It is your duty to protect our Company's intellectual property.

To the extent permitted by law, information and materials that one develops as an employee or creates using Company resources are considered the intellectual property of the Company and an employee must disclose such intellectual property to the Company. The Company reserves the right to protect its intellectual property through the appropriate legal avenues. If applicable law considers you the owner of the intellectual property, then you hereby assign all title and intellectual property rights to the Company, all such rights are hereby owned by the Company, and you have an obligation to help the Company protect its ownership of such rights. Where permitted by applicable law, intellectual property created for the Company by contractors or agents is the property of the Company as a work-for-hire.

The Company has an obligation to respect the intellectual property of Third Parties. Prior to use of any intellectual property, the Company must either purchase the intellectual property, or obtain written permission to use it. An employee should neither copy nor distribute Third Parties' materials that are subject to intellectual property rights and shall comply with all terms and conditions of licenses and other agreements that govern the use of Third Party intellectual property. An employee should report any unauthorized use of the Company's or Third Parties' intellectual property as well.

The Company's policies regarding the use of intellectual property extend to the use of social media. Employees should not use social media to post intellectual property of the Company, including logos, copyrights, patents, trademarks, service marks, trade secrets, processes, innovations, content and software, unless

necessary authorization has been obtained. Nothing in this policy is intended to interfere with, restrain or prevent employee communications protected by state or federal law, including but not limited to communications regarding wages, hours, benefits, or other terms and conditions of employment. Covered persons have the right to engage in or refrain from such activities.

## Electronic Communications

All Company electronic communication systems are business equipment and are the exclusive property of the Company and are intended for authorized Company business. Employees are responsible for using the Company's electronic communications systems and business equipment properly; unauthorized personal use is expressly prohibited, unless the personal use is limited in duration, does not interfere with an employee's work, is consistent with other Company policies, and is not for purposes of facilitating other business ventures. Employees are reminded to always conduct themselves in a professional manner when using electronic communications systems and business equipment. Employees do not have the right of personal privacy in any matter stored on the Company's electronic communications system or business equipment, and the Company reserves the right to monitor any and all aspects of the use of its systems and equipment. The Company does not permit use of unlicensed, illegally or fraudulently obtained, or undocumented software on any Company-owned system or employee-owned system that is used to facilitate Company business.

## 8. Administration of this Code

The Audit Committee has approved this Code. The effective date of this code is September 22, 2021. The Audit Committee must approve any amendments to this Code.

All employees shall review and acknowledge receipt of this Code at the time of hiring and at such other times as determined by the Company. You will be required to certify that you have read, understand, and agree to comply with the Code and that you are not aware of any violations of the Code that you have not reported.

Oversight and administration of this code shall be the responsibility of the Counsel of Corporate Ethics and Compliance. Any violation of this Code may result in disciplinary action up to and including termination.

If you have questions regarding this Code, or Company policies and procedures or applicable law, you are encouraged to contact your manager, People & Culture, the Counsel for Corporate Ethics and Compliance or the Chief Legal and Risk Officer of the Company. Your adherence in complying with and supporting this Code will contribute greatly to our Company's success.

In the unusual circumstance that you believe you may need a waiver of particular provisions of this Code, you should contact the Chief Legal and Risk Officer of the Company. Any amendments to or waiver of this Code for executive officers or directors may be made only by the Board of Directors of the Company and if required by law or applicable stock exchange regulation, will be promptly disclosed to the public.