BITSIGHT

BitSight Technologies, Inc.

CODE OF CONDUCT AND ETHICS

AS OF MAY 22, 2025

Introduction

Since its founding over a decade ago, Bitsight's employees have proudly upheld the company's reputation for the highest standards of business conduct. Bitsight's Code of Conduct and Ethics (the "Code") establishes the guiding principles we expect each employee to follow. Although no Code can anticipate every specific issue you may face or cover every applicable law, by providing you with these guiding principles and illustrative examples, the Code is designed to assist you in identifying and resolving troublesome issues, as well as to advise you where to go for help and advice. While situations can sometimes present unique or complex challenges, when in doubt, you should choose disclosure and transparency. Above all else, Do the Right Thing.

All Bitsight employees have a shared responsibility to speak up and report any behaviors or actions inconsistent with this Code. Reports of Code violations will be treated confidentially to the extent possible, and no person who reports a possible violation in good faith will be subject to retaliation. If you have a question or concern about what is appropriate behavior for you or anyone else, please raise it through one of the many options outlined in the Code.

Please take the time to read and understand this Code. You are expected to apply the Code and its principles to your everyday business activities. In doing so, you are helping Bitsight to grow and remain the standard for providing trusted data and insights that enable risk-based decision making for the world's insurers, investors, enterprises, and governments, which is rooted in our shared commitment to integrity and trust – a source of pride for all of us and a driver of our continued success.

Complying With the Letter and Spirit of the Law

Bitsight and its employees are required to comply with all laws, rules, and regulations applicable to Bitsight.

You must not take any action on behalf of Bitsight or its subsidiaries that violates any law or regulation. Not only is this important to avoid the consequences of legal violations that can include heavy fines, jail terms, expensive lawsuits, and termination of your employment, it is also good business practice.

If you become aware of any violation of law, rule, or regulation by Bitsight or by any team member, please report the violation promptly to your manager, the Human Resources ("HR") Department or the Legal Department. You may also report the violation to the Anonymous Reporting Hotline (refer to the "Where to Seek Help and Report Concerns" section at the end of the Code for contact information). We always strive to address matters internally where practical, but you should not feel discouraged from reporting any illegal activity to an appropriate government or regulatory authority.

Observing Ethical Business Standards and Protecting Bitsight's Reputation

As a Bitsight employee, you must strive to maintain the highest standards of personal ethics and integrity in your dealings on behalf of Bitsight and not act in a manner that would harm Bitsight's reputation. At a minimum, this means complying with the principles and policies articulated in this Code, and upholding Bitsight's core values.

Bitsight's Core Values

- **Integrity** – We have a moral compass that does not waver.
- **Curiosity** – We actively seek out challenges and experiences.
- **Community** – We look after each other and our diverse communities.
- **Excellence** – We strive to be the best that we can.
- **Humility** – We credit our success to the team and are open minded.

How We Treat Our Colleagues

Equal Opportunity Employer

Bitsight is committed to providing a work environment that is free of discrimination and harassment on the basis of race, color, national origin, sex, gender, gender identity or expression, sexual orientation, marital status, registered domestic partner status, citizenship status, religion, age, physical or mental disability, medical condition, genetic characteristics and information, ancestry, military and veteran status, or any other protected category. We provide equal employment opportunity to all individuals in compliance with all legal requirements.

Bitsight is also committed to fostering an inclusive workplace where talented people work, thrive, contribute to Bitsight's success, and develop their careers and the careers of our colleagues. Supporting a diverse, engaged workforce allows us to be successful in building trust, empowering teams, and serving our customers.

Discrimination and Harassment is Prohibited

Discrimination and harassment, including sexual harassment and discriminatory harassment, violate the laws of most jurisdictions around the world and are strictly prohibited by Bitsight. This prohibition applies to all discrimination and harassment affecting the work environment, whether it occurs in the office, outside the office (e.g., at customer-related, Bitsight-related, or after-hours events), or through the use of electronic communications, including electronic mail, voice mail, text messages, collaboration tools, social media, and the Internet, even if such use occurs on personal devices and during non-work hours.

Bitsight prohibits discrimination and harassment not only as to employees, but also as to applicants for employment, interns, visitors, customers, vendors, and contractors providing services to Bitsight in the workplace. A harasser can be a superior, a subordinate, a coworker, or anyone in the workplace including an independent contractor, contract worker, vendor, customer, or visitor.

Discrimination and harassment by non-employees (e.g., customers, independent contractors, vendors) is also prohibited.

What is Sexual Harassment?

Sexual harassment includes harassment based on sex, gender, sexual orientation, gender identity, gender expression, and the status of being transgender. Sexual harassment includes unwelcome sexual conduct, including sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature, or which is directed to an individual because of that individual's sex, when:

- submission to such conduct is either explicitly or implicitly made a term or condition of an individual’s employment;
- submission to or rejection of such conduct is used as the basis for employment decisions affecting the individual; or
- such conduct has the purpose or effect of unreasonably interfering with an individual’s work performance, violating an individual’s dignity, or creating an intimidating, hostile, or offensive working environment.

Sexual harassment is prohibited without regard to the sex of the individual being harassed, whether the individual engaged in harassment and the individual being harassed are of the same or different sexes, or whether the employee accepts or rejects the advance. Employees should be aware that, in addition to being contrary to Bitsight policy, sexual harassment can violate the law and that employees who engage in such conduct may be held personally liable pursuant to local laws.

Examples of what may constitute sexual harassment include: threatening or taking adverse employment actions if sexual favors are not granted; demands for sexual favors in exchange for favorable or preferential treatment; unwelcome flirtations, propositions or advances; unwelcome physical contact such as pinching, patting, kissing, hugging or grabbing; whistling, leering, improper gestures or offensive remarks, including unwelcome comments about appearance; sexual jokes, or inappropriate use of sexually explicit or offensive language; displaying sexually suggestive objects or pictures in the workplace; hostile actions taken against an individual

because of that individual's sex, sexual orientation, gender identity, gender expression, or the status of being transgender; sex stereotyping; and sexual assault, sexual battery, or attempt to commit these acts. The foregoing list is not intended to be all-inclusive.

What Other Conduct is Considered to be Discriminatory Harassment?

"Other discriminatory harassment" includes verbal or physical conduct that denigrates or shows hostility or aversion toward an individual because of his or her race, color, sex, gender, age, religion or religious creed, national origin, ancestry, citizenship, marital status, sexual orientation, gender identity, gender expression, genetic information, physical or mental disability, military or veteran status, or any other characteristic protected by law, and that:

- has the purpose or effect of creating an intimidating, hostile, or offensive work environment; or
- has the purpose or effect of unreasonably interfering with an individual's work performance.

Examples of what may constitute such harassment include: using epithets or slurs; threatening, intimidating, or engaging in hostile acts that focus on a protected characteristic, including jokes or pranks; and placing or circulating anywhere on Bitsight premises, or using Company resources, including electronic mail, voicemail and the Internet, to create, send, receive, or store written or graphic material that denigrates or shows hostility, bias against or aversion toward a person or group because of a protected characteristic. The foregoing list is not intended to be all-inclusive.

Nepotism

To avoid the appearance of conflicts of interest or favoritism in the workplace, subject to applicable law, Bitsight places restrictions on the hiring and transfer of individuals in a close personal relationship with employees. Therefore, relatives of or individuals otherwise in a close personal relationship with current employees — including spouses, domestic partners (or other individuals cohabiting with and sharing financial responsibilities with the employee), individuals with whom employees share a romantic and/or sexual relationship, parents, stepparents, brothers, sisters, brothers/sisters-in-law, children, stepchildren, grandparents, grandchildren, mothers/ fathers-in-law, sons/daughters-in-law, aunts, uncles, nieces, nephews, and a domestic partner's parents, siblings, or children — will be considered for employment and job placement only under certain circumstances.

Hiring managers who believe there may be an actual or perceived conflict of interest based on this nepotism policy with respect to a candidate should notify the Human Resources Department to discuss the circumstances before engaging with such a candidate.

Employee Mobility

Bitsight must comply with income tax, employment and other laws and regulations of states, municipalities, and countries from which its employees perform work on the Company's behalf. In addition, all countries regulate the entry of citizens of other countries and the rights of persons from other countries to work there. Accordingly, employees must receive approval from their manager and HR Business Partner before changing their place of residence or otherwise

working from another state, territory, or country for more than 90 calendar days in any given year.

Employment Verification and Reference Requests for Current and Former Employees

To protect the privacy of Bitsight's current and former employees, all requests for verification of employment or references concerning current and former Bitsight employees should be directed to Bitsight's HR Department.

Health and Safety

Bitsight is committed to protecting the safety, health, and well-being of all employees and individuals in our workplace, and we expect our employees to take reasonable care to further those efforts. As a result, we are committed to complying with all environmental, health and safety laws, and regulations of all countries and localities in which we do business. Bitsight believes it is our obligation to respect the environment in the worldwide communities where we operate and live. We strive to operate in a way that protects and preserves our environment and natural resources and maintains a healthy, safe, and environmentally sound workplace.

Bitsight will not tolerate acts of workplace violence by directors, employees, customers, visitors, vendors, consultants, temporary workers, or other individuals doing business with Bitsight, including behaviors that abuse, threaten, or intimidate another person and negatively affect the individual, either physically or psychologically. This applies to Bitsight offices, customer-related or Bitsight-related events outside the office, as well as the use of Bitsight's technology resources (as further defined in Bitsight's Acceptable Use Policy), including email, voicemail, the Internet, collaboration tools, and any other Company-supported communication channels. If you believe you have been subjected to workplace violence of any kind, you should report the matter to the Human Resources or Legal Departments.

All Bitsight employees are expected to conduct business free from the influence of any substances that impair their ability to work safely and effectively, including alcohol, illegal drugs, and controlled substances, including, in certain circumstances, prescription medication. In addition, the manufacture, distribution, dispensation, or possession of illegal drugs in Bitsight offices or while performing work for Bitsight is prohibited. While Bitsight recognizes that there might be times when alcohol is served at Company-sponsored events or business-related meals or social functions, individuals are expected to consume alcohol in moderation and to act professionally and responsibly at all times. Be aware that local policies and laws may provide additional guidance governing the possession and use of drugs and alcohol at work in a particular location, and employees are expected to know and follow all applicable policies and laws.

Protection of Personal Data

As a cybersecurity industry leader, Bitsight values and protects its employees personal data, and takes operational and technological measures to protect it from misuse or disclosure. Bitsight also strives for transparency in how employees information is used for legitimate business purposes.

For Bitsight employees outside of the United States, please be advised that your data may be transferred to, stored, and processed by other members of the Bitsight group of companies, external agents, or contractors in countries outside of your jurisdiction, which may not have similar data protection laws as your jurisdiction. However, your personal data will only be transferred to recipients that have confirmed an adequate level of protection for the security of your data.

Depending on the jurisdiction in which you are employed, you may receive separate documentation regarding the processing of personal data, such as an employee personal data notice or consent form. If you receive such documentation, that document will supersede the information set out in this section, and you should refer to that document, rather than this section of the Code, for information about the processing of your personal data.

If you would like any further information about the collection and processing of your personal data, including any rights you may have under local law to access, modify, update, correct, or delete such personal data, please contact the HR Department.

Bitsight likewise values and protects personal data received from customers, vendors, contractors, and other third parties, and employs stringent information security measures to avoid misuse or disclosure of such data. These include undergoing a SOC 2 audit for its own business systems, adhering to the European Union - United States (U.S.) Data Privacy Framework program (EU-U.S., Swiss-U.S., and UK Addendum), and receiving Asia-Pacific Economic Cooperation Cross- Border Privacy Rules (APEC CBPR) and Asia-Pacific Economic Cooperation Privacy Recognition for Processors (APEC PRP) certifications. You are personally responsible for securing, protecting and maintaining the confidentiality of any personal data you access during the course of your relationship with Bitsight in accordance with the Bitsight Acceptable Use Policy, the Bitsight Information Security Policy, and any other Bitsight policies or guidelines on security, as well as applicable laws. If you have any questions about the protection of customer, vendor, contractor, or other third-party personal data, please consult the Legal Department.

Photographs, Videos and Recordings

Bitsight believes in transparency, which includes sharing photos and recordings of Company events and activities with the broader community. Therefore, subject to applicable law, Bitsight may take photographs, video and make audio and/or visual recordings of our employees, and use such photographs, videos, or recordings (including those taken or recorded by third parties), for any use in connection with Bitsight's business in its internal or external materials, including but not limited to electronic and print formats as well as on Bitsight's intranet and external websites, and on social media. Bitsight will use reasonable efforts to inform you when you are participating in a Bitsight event that is being photographed or recorded. By participating in such events, to the extent permitted by applicable law, you consent to being photographed and recorded and to Bitsight's use of such photographs and recordings of you as described above at any time.

However, to prevent disclosure of confidential information, to protect the privacy of employees, customers and other third parties, and to prevent sexual and other harassment in the workplace or otherwise, Bitsight prohibits employees from engaging in any type of surreptitious and/or

unauthorized video and/or audio recording or photography while employees are engaged in Bitsight's business. In addition, local laws in many jurisdictions prohibit photography, video and/or audio recording without permission from the party being recorded.

How We Protect the Company and its Shareholders

Bitsight requires its employees to conduct themselves according to the highest standards of integrity and ethics in all of their business activities. Besides being the right thing to do, ethical conduct is good business practice because it is essential for maintaining trusting relationships with our customers. Business conduct is also regulated by many laws relating to fraud, deceptive acts, bribery and corruption, consumer protection, competition, unfair trade practices, and property, including intellectual property such as patents, trademarks, and copyrights.

Honest and Ethical Conduct and Fair Dealing

Bitsight depends on its reputation for integrity. The way we deal with our customers, business partners and competitors shapes our reputation, builds long-term trust and ultimately determines our growth and success. You should deal fairly with Bitsight's customers, business partners, competitors, and employees. We must never take unfair advantage of others through manipulation, concealment, abuse of information, misrepresentation of material facts, or any other unfair dealing practice.

Antitrust and Competition

Bitsight is committed to comply with the antitrust and competition laws of any country that apply to Bitsight's business. Bitsight will not tolerate any business transaction or activity that violates those laws. The general aim of antitrust laws is to promote free and open competition based on quality, price, and service. Free and open competition requires that we refrain from: collaborating or communicating with any competitor in any way that might injure competition; securing, threatening to secure, or maintaining a monopoly through anticompetitive means (in the United States) or "abusing a dominant market position" (in other jurisdictions); or otherwise harming normal competition.

Antitrust violations can result in very large corporate fines, as well as fines and jail terms for individuals. Antitrust laws in certain jurisdictions allow parties injured by an antitrust violation to recover substantial damage awards.

Antitrust laws are deliberately broad and general in their language. They contain sweeping provisions against restraints that threaten a competitive business economy, but they provide no definitive list of those activities. This means we must pay careful attention to possible antitrust implications of Bitsight's business activities. Bitsight's Legal Department should be contacted in all cases of doubt.

Deception and Fraud

You must not engage in any form of fraud or deception with a customer, the Company, or any other party. The basis of deception or fraud is a misrepresentation, which in its simplest form is a statement that is not true or is misleading. To avoid any suggestion of deception or fraud, you should note the following:

- Representations as a whole can be misleading, even though each statement considered separately is literally true.
- Failure to disclose important additional or qualifying information may be a misrepresentation.
- Representations should not shade the truth.
- Representations should not claim characteristics for a product or service that it does not have.

Representations concerning the factual characteristics of products and services of Bitsight and its competitors must be capable of being proven.

Maintaining Accurate Business Records

It is imperative that the Company maintain accurate business records. Company business records must always be prepared accurately and reliably, reflect the true nature of the transaction, and be stored properly. All transactions must be executed in accordance with the Company's general or specific authorization. The Company's books, records and accounts must reflect all transactions and all other events of the Company that are the subject of a specific regulatory record-keeping requirement or Company record-keeping policy. Accurate business records are also required to allow the Company to fulfill its obligation to provide full, fair, timely, and understandable financial and other disclosure to stockholders, and governments of the countries in which we do business.

It is critical that no one creates or participates in the creation of any records that are intended to mislead anyone or conceal anything. Examples of such conduct include making records appear as though payments were made to one person when, in fact, they were made to another, submitting expense reports that do not accurately reflect the true nature of the expense, or submitting inaccurate sales results to the Accounting Department. Any employee who creates or participates in the creation of misleading or falsified records will be subject to disciplinary action up to and including termination.

The financial and other books and records of the Company must not be falsified. Anyone having information or knowledge of any hidden fund or asset, of any false or artificial entry in the Company's books and records, or of any inappropriate payment, should promptly report the matter to the Chief Financial Officer and the Legal Department, or via the Anonymous Reporting Hotline. Submitting false financial results of any kind violates this Code and can result in fraud charges against the Company.

Conflicts of Interest

Your obligation to conduct Bitsight's business in an honest and ethical manner includes the ethical handling of actual and potential conflicts of interest between personal and business relationships.

A conflict of interest exists when your personal interest interferes in any way with Bitsight's interests.

Actual or potential conflicts of interest can arise in a variety of circumstances. Below, the Code addresses several ways in which conflicts of interest can arise, including: Interests in Outside

Companies; Positions with Outside Entities; and Accepting Gifts, Entertainment or Other Things of Value. In addition to those situations discussed in further detail below, below are some additional examples of situations that can create actual or potential conflicts of interest:

- **Improper Personal Benefits** – Conflicts of interest arise when an employee, or a member of their family, receives improper personal benefits as a result of their position in Bitsight. Such personal benefits can take a variety of forms, including discounts, opportunities, or other advantages. You may not accept any benefits from the Company that have not been duly authorized and approved by the Company.
- **Personal Relationships** – A conflict of interest may arise from the personal relationship of a Bitsight employee with an employee of a customer, issuer, vendor, or other business contact. If you have or become involved in any such a relationship, subject to applicable law, you should notify your manager and a member of the Legal Department, who will assess the situation and advise you whether any steps must be taken to mitigate the conflict.
- **Prior Employment** – an employee's recent employment at a customer, issuer, vendor, Bitsight external auditor, or other business contact can create an actual or potential conflict of interest with the employee's job duties at Bitsight. As a result, employees may be required to refrain from participating in certain professional activities relating to that prior employer.

Employees are required to disclose any actual or potential conflicts of interest so the Company can determine what, if any, action to take to mitigate the conflict. If you have any questions regarding whether a particular situation may create a conflict of interest, please discuss the situation with your manager or contact the Legal Department.

Corporate Opportunities

Employees owe a duty to Bitsight to advance its legitimate interests when the opportunity to do so arises. If you learn of a business or investment opportunity through the use of corporate property or information or your position at Bitsight, such as from a competitor or actual or potential customer, supplier or business associate of the Company, you may not participate in the opportunity or make the investment, or assist another person in so doing, without the prior written approval of the General Counsel. Such an opportunity should be considered an investment opportunity for the Company in the first instance. You may not use corporate property or information or your position at Bitsight for personal gain, and you may not compete with the Company, nor may you assist someone else in doing so.

Interests in Outside Companies

Decisions to do business with individuals or companies must be made solely on the basis of the best interests of the Company.

You should not participate in the selection of vendors, business partners or contractors, or make any decisions as part of your job (including servicing a customer account) for any entity, if you or an immediate relation has a significant business interest in such entity.

You should not acquire a significant business interest in any entity that may create an actual or potential conflict with your duties on behalf of Bitsight, unless you obtain approval first from your manager or supervisor and then have your request reviewed by the Legal Department.

Positions With Outside Entities

A Bitsight employee serving as an officer or director of an outside company may be regarded as a representative of Bitsight and might find their duties with that company to be in conflict with Bitsight's interests. Employees may not accept such a position unless and until they have received approval first from their manager or supervisor and have their request reviewed by the Legal Department, subject to applicable law.

An employee should not take a part-time or second job or any position with an outside entity, including not-for-profit entities, that may create a conflict of interest or interfere in any way with the duties that the employee performs for the Company. Before accepting any outside employment or other position, whether paid or unpaid, at an outside entity, you should discuss first with your manager or supervisor whether such a position would present a conflict of interest.

Solicitation of Co-Workers for Personal Gain

Solicitation by employees of other Bitsight employees or customers for personal gain is prohibited. This principle applies whether the employee is on working time, on a break, or at lunch. Employees also may not use Company resources, including telephones, fax machines, and computers, to engage in an outside business activity.

Accepting Gifts, Entertainment or Other Things of Value

The receipt of gifts, entertainment, or other things of value from entities or persons who do or are seeking to do business with Bitsight can influence, or appear to influence, your business judgment, can create actual or potential conflicts of interest, and could lead to inferences of bribery under the laws in certain jurisdictions. For these reasons, Bitsight limits the types of gifts, entertainment, or other things of value employees may accept from such business contacts.

Certain types of gifts, entertainment, or other things of value are always improper, and therefore may not be accepted at any time. Specifically, you are prohibited from accepting:

- any gift, entertainment, or other thing of value, regardless of its value, where there is any reason to believe that it is being offered in an attempt to influence your work at Bitsight;
- any gift, entertainment, or other thing of value that is extravagant or lavish in nature, or which exceeds local social or business custom; and/or
- any gift, entertainment, or other thing of value that is intended to be concealed or is not offered openly and transparently.

Finally, you should never solicit or encourage any business contact to offer you a gift or other thing of value.

Subject to the above limitations and applicable law, all Bitsight employees are permitted to accept the following gifts, entertainment, or other things of value:

- Occasional non-cash business gifts of nominal value (less than or equal to US $100 per gift or the relevant local equivalent). The total value of such gifts from any business contact may not exceed US $500 in any 12-month period.

- Customary and reasonable meals and entertainment at which the non-Bitsight business contact also is present, such as an occasional business meal or sporting event, where there is a legitimate business purpose.

Employees should be guided by the below examples when determining whether it is appropriate to accept a gift, entertainment, or other thing of value:

- A promotional ballpoint pen would be of nominal value, but a gold wristwatch would not be acceptable.
- A holiday gift of a bottle of wine from a vendor or customer would be of nominal value (provided it is worth $100 or less), but a case of fine champagne would not be acceptable.
- Tickets to an ordinary sporting event, which you attend with a business contact, would be considered customary and reasonable, but tickets to the World Cup, Super Bowl, or other similar major sporting event would be considered excessive in value and should not be accepted.
- Ordinary business meals are acceptable, but a lavish dinner at a Michelin star restaurant likely would not be. Good judgment would also dictate that Bitsight should periodically assume the cost of the meal as a business expense.

If you are offered a gift, entertainment, or other thing of value, and you have any question about the appropriateness of accepting it, you should seek guidance from the Legal Department prior to acceptance.

Gifts, entertainment, or other things of value that do not meet the requirements outlined above should be returned to the donor as tactfully as possible. You may refer to this Code when you return such a gift, and you should report such a gift to your manager and the Legal Department.

Finally, laws and customs of some countries permit gifts and courtesies beyond those considered customary in the United States, and refusing such gifts or courtesies might be considered offensive in that country. Bitsight employees should consult the Legal Department if they encounter a situation in which the gift, entertainment, or other thing of value exceeds these rules but their refusal to accept would be seen as offensive.

For information regarding the giving of gifts, please refer to the Anti-Bribery and Anti- Corruption section of the Code.

Conferences and Events

Can I accept a free pass to a conference or event hosted or organized by a third party?

Employees may accept free passes and/or fee waivers to conferences/events as long as there is a clear business purpose to the employee attending the conference/event and the free passes and/or fee waivers are not being provided by a vendor providing or seeking to provide services to Bitsight.

I am presenting at a conference. May I accept reimbursement from a third party for my travel, lodging, and other incidental expenses?

You may accept reimbursement for travel-related expenses when you are speaking/presenting

at a conference as these are not considered gifts under the Code. However, such reimbursement (or direct payment of such expenses on your behalf) must (1) be for your individual travel, lodging, meals, and other reasonable expenses, and (2) not be provided by a vendor providing or seeking to provide services to Bitsight. You should not accept reimbursement for lavish or extravagant travel, lodging, or other expenses. You also may not be reimbursed for the travel or other expenses of any family members or other non-Bitsight employees who accompany you.

Protecting Bitsight's Intellectual Property Rights

Bitsight's business is built upon unique and valuable intellectual property created by its employees. Therefore, when you perform work for Bitsight, Bitsight owns all intellectual property rights in your work, including but not limited to copyright rights and all patentable inventions. To prevent "taint" by unnecessary exposure to third party patents, you should not attempt to do independent patent research, but rather consult the Legal Department if you have questions about prior art, the legality of pursuing a particular invention, or whether a third party is infringing on a Bitsight patent. Likewise, if you are approached by third parties concerning patent portfolios or patent matters of any kind, you should promptly consult the Legal Department rather than engaging with such parties directly.

Unauthorized Copying and Use of Open Source Software

Generally, it is against the law to make copies of legally protected works of others or to use them without proper permission. Wrongful copying of copyrighted materials can result in personal, as well as Company, liability.

Protected works include most publications, computer software, computer code, video and audio files, and certain databases. In addition, protected works may include material displayed or published on web sites, including articles, musical recordings (such as MP3 files), HTML code, graphic designs, photographic images, and audiovisual materials.

You must comply with all license or purchase terms regulating the use of any software or SaaS offering that Bitsight acquires or uses. You must not, when preparing any presentation to or publication for Bitsight employees, customers, investors, or other third parties, copy or use any protected works prepared by any other person who is not a Bitsight employee, or was not a Bitsight employee when such material was prepared, unless you: (a) acknowledge the use of such other person's protected works and identify in the relevant presentation or publication, at a minimum, the name of the author, publisher, and owner of the protected works, and (b) obtain the consent in writing of the owner of the protected works if more than an insubstantial portion of the original work is used. Bitsight's Legal Department can assist you in determining whether such written consent is required.

The law does permit in some circumstances certain "fair use" or "fair dealing" of protected works, but this right is limited and reliance on it should be made only in consultation with Bitsight's Legal Department.

Use of open source, freeware, shareware, "copyleft," or other public software code (together, "Public Software") in Company projects may also raise legal issues. Subject to Bitsight's Open Source Policy, if you use Public Software in connection with a Company project, you must

review and be able to comply with its license terms in a manner that is not detrimental to the Company.

Without limiting the foregoing, you must not use any Public Software in a manner that would require the Company to disclose or distribute any of its proprietary software in source code form or otherwise. This includes, but is not limited to, not using any Public Software provided under the GNU Affero General Public License (Affero GNU GPL) or the GNU General Public License (GNU GPL) for Company projects. If you have questions regarding use of Public Software, please consult Bitsight's Legal Department.

Protecting Bitsight's Trade Secrets and Proprietary Information

We must maintain the confidentiality of Bitsight's trade secrets and other proprietary information. Employees and directors may learn facts about Bitsight's business, plans, or operations that Bitsight has not disclosed to its competitors or the general public.

Examples of Company trade secrets and proprietary information may include, but are not limited to, sensitive information such as customer lists, the terms offered or prices charged to customers, non-public algorithms, formulas, or methodologies, marketing or strategic plans, potential acquisitions, or proprietary product designs or product systems developments. Employees may not disclose such information internally within Bitsight except on a "need to know" basis, nor externally except, in connection with their authorized business activities, to parties with whom Bitsight has entered into agreements containing appropriate confidentiality obligations. This restriction applies equally to the trade secrets of our customers. If you have questions about whether disclosure of a particular trade secret or proprietary information to a third party is permitted, please consult the Legal Department.

Use of Company Resources

Bitsight's funds, time, materials, supplies, technology and information resources, including computer systems and voice mail systems, and all information, copies of documents or messages created, sent, received, or stored on these systems are Company property and must not be used to advance your personal interests.

Employees must use the Company's technology resources in accordance with the Bitsight Acceptable Use Policy.

Each of us has a duty to protect the Company's assets and to use them efficiently. Theft, carelessness, and waste have a direct impact on the Company's growth and profitability. We should take measures to prevent damage to and theft or misuse of Company property. Except as discussed below and in the Acceptable Use Policy, Company assets, including Company funds, time, equipment, materials, resources, and information, must be used for business purposes only. Personal calls from office telephones should be kept to a reasonable minimum. Similarly, use of Company's technology resources, including computers and the Internet, for personal matters should be kept to a reasonable minimum, and any such usage must be consistent with the Bitsight Acceptable Use Policy.

In no instances should such personal use of Company telephones or computers interfere with your work commitments. Further, employees may not use Company office space for personal meetings unrelated to Bitsight's business.

Under no circumstances may an employee use the Company's technology resources to transmit, download, display, otherwise disseminate, or condone the receipt of any sexually explicit material or any material containing ethnic slurs, racial epithets, or anything that may be perceived as harassment of others based on their race, color, sex, gender, age, religion or religious creed, national origin, ancestry, citizenship, marital status, sexual orientation, gender identity, gender expression, genetic information, physical or mental disability, military or veteran status, or any other characteristic protected by law. Employees encountering or receiving such material should immediately report the incident to their manager or to the Human Resources Department.

Employees should be aware that, subject to applicable law, they have no proprietary interest in and no reasonable expectation of privacy while using any Company computer equipment, voice mail equipment or Company-provided access to the Internet, including electronic mail, collaboration tools, instant messaging, SMS/text messages, or similar technologies. To the extent permitted by applicable law, Bitsight reserves the right, through the use of automated software or otherwise, on a continuous, intermittent, or ad hoc basis, to monitor, open, read, review, copy, store, audit, inspect, intercept, access, disclose, and delete all computer documents, systems, disks, voice mail, Internet usage records (including any material that employees might seek to access or download from the Internet), system activity, electronic mail of current and former employees, and any other communications transmitted or received through its systems without notice to any employee and at any time. Such activities may be undertaken for a range of purposes, including but not limited to the following: to protect the security of Bitsight documents, data, information, and systems; to maintain quality standards; to provide business continuity and record retention when an employee is absent (for whatever reason) or when an employee has left the Company; to respond to any subpoena, judicial order, or other request of any governmental agency or authority; to investigate where Bitsight has a legitimate and reasonable concern that an employee or former employee has engaged in wrongdoing, unlawful or illegal acts, or may be in breach of Company requirements or policies; or as the Company's business needs may otherwise require. To the extent permitted by applicable law, the results of any such review, audit, inspection, interception, access, or disclosure may be used for disciplinary purposes or in legal proceedings. To the extent permitted by applicable law, your use of Company computer, voice mail, and electronic communications systems constitutes your acknowledgement and understanding of the foregoing rights of Bitsight and your consent to them.

Any employee who wishes to avoid inspection of any private personal data should not use Company equipment for personal matters nor save any private personal data on Company computer storage devices.

When you leave the Company, all Company property must be returned to the Company.

Safeguarding Bitsight's Technology Resources

Employees are responsible for safeguarding their passwords for access to all Company technology resources, including computer equipment, business applications, and voicemail systems. Individual passwords must not be given to others, nor should employees access any account on Company computer, application, or voice mail systems other than their own, except for Bitsight's IT Department in connection with technical support. Employees must safeguard the

laptops, cell phones, or any other technology resources provided to them by the Company and should exercise the highest standard of care reasonable and appropriate to the circumstances to prevent such technology resources from being lost, stolen, or accessed by an unauthorized person.

Bitsight has also installed a number of security features and controls, such as firewalls, proxy servers, and anti-malware software, to protect its technology resources and information. You should never disable or attempt to evade the operation of these security features.

If you suspect or become aware of any unauthorized access to, acquisition of, or loss, damage, or misuse of, any Bitsight technology resources, or information maintained on, or handled by any technology resource, or any other incident in which the security of Bitsight technology resources or information systems may have been compromised, you must immediately report such incident to Bitsight's Information Security Department by email to security@bitsighttech.com.

Use of Personal Electronic Devices

Employees use of any type of personal electronic devices while conducting any Bitsight business is subject to relevant Bitsight policies, including the Bitsight Acceptable Use Policy, and, where relevant, any agreement relating to use of a personal mobile device.

Employees may be permitted to access Bitsight technology resources through personally-owned cell phones and other mobile computing devices using Bitsight approved third-party downloadable software applications (e.g., Slack).

Employees are reminded that affirmatively downloading, copying, saving, creating, or working on any Bitsight files containing Bitsight confidential or proprietary information on any system or device that is not a technology resource that has been approved by Bitsight's IT Department is prohibited.

Communications with Media

We are committed to maintaining honest, professional and consistent internal and public communications. Accordingly, when issuing statements about the Company or providing information to the public, it is important that only authorized persons speak on Bitsight's behalf. All inquiries from members of the media should be referred to the Company's Vice President for Public Relations by emailing press@bitsight.com.

Expert Network Firms

Because of the risk of violating confidentiality obligations in a way that could damage Bitsight’s interests, we strongly discourage employees from speaking with any representatives of expert network firms (e.g., Third Bridge, Gerson Lehrman, Guidepoint, and others). To the extent you believe there is a compelling reason to speak with an expert network firm despite the foregoing, please consult with your Vice President first, and if approved, a member of the Legal Department before having the
conversation. Employees should also not agree to serve as an expert witness in any litigation, arbitration or other legal proceeding without first receiving approval from the Legal Department.

Social Media

Employees who use online communication tools like blogs, social media sites and other digital platforms — whether on their own personal time or in an official capacity on behalf of Bitsight — assume responsibility for ensuring that their activities comply with Bitsight policies as well as all applicable laws and regulations.

Any time we endorse or promote Bitsight or any of our products in a forum in which our connection to Bitsight is not obvious, whether in person or online, we need to disclose our connection to Bitsight. Such disclosure should be clear and conspicuous, readily visible within our communication, and understandable and apparent to the average reader near the beginning of the communication.

If we use social media or other forums to express our personal views regarding Bitsight, our products, or our competitors, we should indicate that our comments do not represent the positions, strategies, or opinions of Bitsight. If we engage or provide something of value to a consultant, agency, celebrity, consumer, blogger, or other party to entice or encourage them to review, promote, or endorse Bitsight or our products, we must require that those parties also disclose their affiliation with Bitsight.

These requirements apply even to comments we make on our own personal blog or social media pages or on third-party websites, as well as to actions we take on Bitsight- affiliated websites, such as product ratings and reviews, and our brands 'social media pages.

Employees as Consultants/Conversion of Consultants to Employees

Current Bitsight employees may not be engaged to work as consultants, as independent contractors or as contract workers for the Company at the same time they are employed. This applies regardless of whether or not the work is related to the duties of the employee's position, and whether or not payment is made outside normal payroll routines.

Further, the Legal Department must approve any situation in which a former Bitsight employee wishes to become an independent contractor or contract worker for Bitsight. In addition, the Legal and Human Resources Departments should be consulted in situations in which an individual who has worked as an independent contractor/contract worker for Bitsight wishes to become a Bitsight employee.

How We Act With Integrity in the Global Community

Insider Trading and Market Abuse

Employees and directors who have access to confidential information are not permitted to use or share that information for purposes of trading securities or for any other purpose except the conduct of our business. The insider trading laws and regulations of the United States and many other jurisdictions prohibit buying, selling, or recommending that someone else buy or sell a company’s securities while in possession of material non-public information about that company. In addition to heavy fines and lengthy prison terms, a violator in the United States or one who trades on a U.S. stock exchange can be required to pay civil penalties of up to three

times the profit gained, or loss avoided, by certain unlawful transactions or disclosures.
Bitsight may also have to pay substantial fines. In other countries, such actions can lead to fines, public censure, compensation/restitution orders, and injunctions, as well as potential prison terms. “Material” information is generally regarded as information that a reasonable investor would think important in deciding whether to buy, hold, or sell a security; in short, it is any information that could reasonably affect the price of the security. In other jurisdictions, “material” information may be referred to as “inside information” or “price- sensitive information.”

Examples of material / inside information may include: sales results; earnings or estimates; dividend actions; strategic plans; new products, discoveries or services; important personnel changes; acquisition and divestiture plans; financing plans; proposed securities offerings; marketing plans and joint ventures; government actions; major litigation, litigation developments, or potential claims; restructurings and recapitalizations; the negotiation or termination of major contracts; and nonpublic information about major security breaches affecting a particular entity.

Anti-Bribery and Anti-Corruption

You must not engage in commercial or public sector bribery. This means you or anyone acting on Bitsight's behalf cannot offer, promise, or give money, business courtesies, or anything else of value, directly or indirectly, to a commercial party or public official intending to receive, or for having received, favorable treatment. You are also prohibited from ''turning a blind eye” to the likelihood that an agent or other third party is or will be making an improper payment in connection with the Company's business.
Anti-corruption laws in various jurisdictions, including the U.S. Foreign Corrupt Practices Act (''FCPA”), the UK Bribery Act 2010 (''UK Bribery Act”) and local country laws where Bitsight operates, restrict companies and employees conduct in this area and subject Bitsight and its employees to serious penalties for violations.

Bitsight also is required to assure that its books and records accurately reflect the true nature of Company transactions, and to maintain internal accounting control systems designed to prevent and detect improper transactions. Accordingly, all information relating to business expenses or other costs incurred on behalf of the Company must be recorded accurately and with sufficient detail.

When is it permissible to give business courtesies to business contacts?

Employees generally may give business courtesies (including gifts) to business contacts, provided that they comply with the following requirements: (1) the cost must be reasonable and justifiable under the circumstances; (2) they must comply with applicable laws; (3) they must not reasonably be interpreted as an attempt to obtain or retain an improper business advantage, and must not reflect negatively on the reputation of Bitsight or the recipient; (4) they must be bona fide and must directly relate to a legitimate business purpose; and (5) they must be supported by receipts and properly documented in accordance with any applicable expense reimbursement and accounting procedures.

No business courtesies may be given, directly or indirectly, to public officials without complying with all of these requirements. Please be aware that employees of publicly

funded institutions (e.g., public universities) may be deemed public officials as well as employees who work directly for local, state, provincial, or national governments. If you have any questions regarding the provision of business courtesies to public officials, you should consult the Legal Department prior to providing them.

Political Activities

Bitsight encourages you to participate in the political process on your own time, as long as you take care not to imply that you are acting on behalf of Bitsight. You should not permit your Bitsight affiliation to be noted in any outside organization's materials or activities without the approval of Bitsight's Legal Department unless you are serving as a Bitsight representative.

Corporations are not permitted to make political contributions in connection with any election involving any United States federal office. There are similar laws in some states and other countries. Your personal contributions must not be made with, or reimbursed by, Company funds in U.S. federal campaigns or in other U.S. or foreign campaigns where it is illegal. Individual participation must be completely voluntary and must occur only during non-working hours. Political activity may not involve the use of Bitsight funds, personnel time, equipment, supplies, or facilities.

Any proposed Company political contribution anywhere should be discussed in advance with Bitsight's Legal Department. Influencing legislation or "lobbying" is also restricted by the laws of the United States, certain states and other countries or subdivisions thereof. Under such laws, Bitsight may be required to register and report if its employees engage in lobbying activities. This may need to be done if you communicate with any members of federal, state, or local legislative or executive office in the U.S. or members of legislative or executive office or other public officials in other jurisdictions for the purpose of influencing any action on the Company's behalf. Before any employee takes a public position on government actions on behalf of the Company, Bitsight's Legal Department should be consulted. Employees who serve on government advisory boards should also be aware of applicable restrictions on their ability to promote Bitsight's business in conjunction with their work on such boards.

Economic and Trade Sanctions and Export Compliance

Bitsight complies with all economic sanctions-related laws and regulations and export controls in jurisdictions in which it operates. Economic sanctions rules prohibit or restrict trade with certain individuals, entities, nations, or industries. You must not engage in any prohibited dealings, including transacting with or providing services, directly or indirectly, to:

- Any individual or entity located, organized, or ordinarily resident in a comprehensively sanctioned jurisdiction;
- Any entity 50 percent or more owned by a person or persons located in a comprehensively sanctioned jurisdiction; or
- Any person subject to blocking or asset freeze sanctions, including entities owned 50 percent or more by a person or persons subject to blocking or asset freeze sanctions.

Economic sanctions are generally divided into three types:

- Comprehensive embargoes imposing restrictions on a particular geography (or persons located therein), which under the U.S. sanctions regime currently includes Iran; Syria; the Crimea, Donetsk, and Luhansk Regions of Ukraine; North Korea; and Cuba;
- “List-based” sanctions which impose prohibitions on transacting with certain persons identified on watchlists, such as the list of Specially Designated Nationals and Blocked Persons (“the SDN List”) maintained by the U.S. Treasury Department’s Office of Foreign Assets Control (“OFAC”) or the Consolidated List of Financial Sanctions Targets in the UK maintained by the Office of Financial Sanctions Implementation (“OFSI”); and
- “Sectoral” sanctions, which impose more limited restrictions on persons conducting certain activities in certain sectors.

The export or re-export of goods, including software utilizing encryption technology, may be subject to regulatory requirements.

You should contact Bitsight Legal Department if you are:

- Unclear if you can do business with a particular country, entity, or individual based on economic sanctions;
- Unsure of export controls applicable to goods/technology/software; particularly encryption technology to a country outside the United States; or
- In need of information regarding local export laws.

You should also bear in mind that anti-boycott laws may apply in the United States or other countries in which Bitsight does business (e.g., laws that prohibit cooperation in a boycott against Israel or another third country). You must contact the Bitsight Legal Department to resolve conflicts arising in connection with anti-boycott laws and immediately inform the Legal Department of any boycott-related requests that you receive as part of a customer contract or otherwise.

Anti-Money Laundering

Bitsight will not accept any payments that appear to derive from money laundering in any form. Money laundering is the act of disguising illegally- gained funds so that they appear to come from legitimate sources. Typically, it involves three steps. First, the illegally- gained funds are introduced into a legitimate financial system. Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts. Finally, it is integrated into the financial system through additional transactions until the illegally-gained funds appear to be ''clean.”

If any Bitsight employee has reason to believe that any customer is deriving its funds from illegal activity or engaging in any effort to conceal or disguise the nature, location, source, ownership, or control of funds that will be paid to Bitsight or in connection with a transaction in which Bitsight is involved, this should be reported immediately to Bitsight's Legal Department.

Business in New Countries

The decision to expand Company operations into any country other than those in which we are

qualified to do business may carry important legal and tax implications. Before undertaking business in any new country, including selling into any new country or permitting employees or contract workers to conduct remote work from such country, you should consult the Legal Department about any issues that arise under these and other laws that apply to your job.

Government Investigations

Bitsight cooperates as appropriate with investigations by the U.S. government, the governments of U.S. states and municipalities, the governments of other countries, and their departments and agencies or judicial authorities. Bitsight employees must never:
(i) destroy, hide or alter any document or part of a document in anticipation of a request for those documents from a government agency or a court; (ii) lie or make any misleading statements to any government investigator, or in any deposition or other testimony; or (iii) attempt to influence an employee or any other person to engage in any of these acts.

Although Bitsight cooperates as appropriate with governmental investigations and responds properly to valid legal process, Bitsight also has legitimate and important interests to protect. For example, Bitsight has important confidentiality obligations to its customers, including the obligation, in certain instances, to provide notice to those customers when requested or ordered to provide information about them. To assist Bitsight in complying with our obligations to our customers or others, and to verify the accuracy of the information we provide, you should notify the Legal Department if you are approached by a government investigator regarding Bitsight or any of its customers.

This should in no way deter you from reporting any suspected wrongdoing at the Company to Bitsight's Anonymous Reporting Hotline, the Legal Department, or any of the other resources identified in this Code. Nothing herein or in any Bitsight agreement shall limit your right to provide truthful disclosures to governmental and/or regulatory authorities that are protected under the whistleblower provisions of any applicable law or regulation. Bitsight prohibits retaliation against any employee for making a good faith report of suspected wrongdoing to the Company or the government, or for cooperating with a government investigation. If you believe that you have been subject to retaliation for making a good faith report or for cooperating with a government investigation, you should report the matter to the Legal Department immediately. Alternatively, you may report the matter to Bitsight's Anonymous Reporting Hotline.

Civil Litigation

Like all companies, Bitsight is sometimes involved in civil litigation, and you may be approached by lawyers for companies or people who have brought suit or may be thinking of bringing suit against the Company or one of our customers. You should contact the Legal Department before responding to any questions about Bitsight or our customers from lawyers or representatives of third parties who may be involved in or contemplating bringing a lawsuit against Bitsight or our customers. Please be aware that you must contact the Legal Department before providing such people with any information or records regarding Bitsight or our customers.

Record Retention and Preservation Directives

Documents and other records (in whatever form) must be retained for the periods of time specified by law and under Bitsight's record-retention policies, procedures, and rules.

Under relevant circumstances relating to a government investigation and/or a civil litigation, Bitsight will issue a record preservation directive to all employees who are likely to have in their possession records relevant to the subject matter of the investigation or litigation. Thus, from time to time, you may receive directives from the Legal Department directing you to preserve all such records in your possession or under your control. If you receive such a directive, you must not destroy or otherwise discard any records relating to the subject matter described in the directive, regardless of the place or way those records are stored. If you have not received a record preservation directive but believe you have records related to a subpoena or pending or contemplated litigation, government investigation, or other proceeding, you must immediately contact the Legal Department. In such circumstances, you must also retain and preserve all records that may be responsive to the subpoena or relevant to the litigation or to the investigation until you are advised by the Legal Department as to how to proceed. In addition, if you learn of a subpoena or a pending or contemplated litigation or government investigation, you must immediately contact the Legal Department.

You must also affirmatively preserve from destruction all relevant records that without intervention would automatically be destroyed or erased (such as voice mail messages). Destruction of such records, even if inadvertent, could seriously prejudice the Company. The destruction or falsification of a record with the intent to impede or that has the effect of impeding a governmental investigation, audit or examination may lead to prosecution for obstruction of justice. If you are not sure whether a record can be destroyed, consult Bitsight's Legal Department before doing so.

These retention obligations apply equally to Company records that you store in locations outside Bitsight's offices, including your home. Thus, if you have any records outside Bitsight's offices, you will be expected to provide any such records to the Legal Department upon request. Furthermore, notwithstanding the other provisions of this Code, if you have any electronic records on your personal computer, smartphone, tablet or other electronic device, subject to applicable law, you may be asked to provide Bitsight with access to such personal electronic device so that the Legal Department or an agent thereof may extract any Bitsight records related to an ongoing investigation and/or litigation.

Combating Trafficking in Persons

Bitsight and the United States Government, as well as other international governments, strictly prohibit trafficking in persons, defined to mean the recruitment, harboring, transportation, provision or obtaining of a person for labor or services, through the use of force, fraud, or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery and sex trafficking. Any violation of these policies, or any international laws or regulations including, but not limited to, the UK Modern Slavery Act of 2015, could result in disciplinary action, including termination of employment.

Code Administration

Interpretation

Bitsight has implemented policies concerning legal and ethical behavior in various areas. The Code is not intended to supersede those policies, but to provide a summary of Bitsight's

policies and expectations in certain areas. Employees should read the Code together with Bitsight's other policies.

Bitsight's General Counsel is responsible for interpreting and applying the Code to specific situations when questions arise. Any questions relating to how the Code should be interpreted or applied should be addressed to Bitsight's Legal Department.

The Code cannot cover all the legal requirements of each jurisdiction in which the Company does business. Because Bitsight is a United States corporation, particular attention is given to U.S. legal requirements. This Code, however, applies to all employees of Bitsight Technologies, Inc. and all employees of its wholly-owned subsidiaries worldwide, including part-time and limited duration employees. The terms "Bitsight" and "the Company" are used in this Code to refer to Bitsight Technologies, Inc. and its wholly-owned subsidiaries.

This Code is not intended to and should not be construed to prevent you from engaging in concerted activity protected by the rules and regulations of the U.S. National Labor Relations Board (or government labor agency or board in your jurisdiction) or any other federal or state agency, or from testifying, participating, or otherwise assisting in any federal or state administrative, judicial, or legislative proceeding or investigation.

Investigations of Suspected Violations

Bitsight will conduct a prompt, fair, and impartial investigation of all reports of suspected violations of the Code. Employees are required to cooperate as needed in investigations. Investigations may be conducted by members of the Legal Department, the HR Department, or outside professionals engaged for this purpose. While investigations may vary from case to case, they generally will include:

- conducting a review of the allegations;
- assessing whether any interim actions to protect the complaining party are necessary;
- conducting interviews of relevant parties;
- obtaining and reviewing relevant documents; and
- preparing a written report.

Bitsight will then make a determination based on all evidence collected and will maintain the confidentiality of the investigation to the extent reasonably possible and as permitted by applicable laws. Bitsight will also keep written documentation and associated documents in its records.

Upon completion of an investigation, Bitsight will notify the person(s) who raised the concern and the subject(s) of the investigation's conclusion. Given requirements under data protection laws in certain jurisdictions, Bitsight may be obligated to inform the subject of a complaint that the complaint was filed, and how he or she can exercise his or her right to access and correct the information. The subject of the complaint will not be provided information identifying the person who reported the allegation unless required by local law.

If Bitsight determines that a violation of the law or the Code has occurred, Bitsight will take appropriate corrective and/or disciplinary action, up to and including termination, as warranted

by the circumstances and regardless of the seniority of the individuals involved, subject to applicable law. If, during an investigation, Bitsight also determines that any manager knew of inappropriate conduct and failed to report the conduct, Bitsight will take appropriate corrective and/or disciplinary action, up to and including termination, subject to applicable law.

Employees and managers should not conduct their own preliminary investigations. Investigations of suspected violations may involve complex legal issues, and acting on your own may compromise the integrity of an investigation and adversely affect both you and the Company.

Enforcement of the Code

The principles set forth in this Code and other relevant Company policies and procedures will be enforced at all levels of the Company. The Company intends to use every reasonable effort to prevent conduct not in compliance with this Code and to halt any such conduct that may occur as soon as reasonably possible after its discovery. Subject to applicable law and agreements, Company personnel who violate this Code and other Company policies and procedures may be subject to disciplinary action, up to and including termination.

In some cases, compliance with the Code and other Company policies will be monitored by periodic audits, investigations or other reviews. In connection with any such audits, investigations or reviews, you are required to cooperate fully, provide truthful and accurate information, and respond to requests for certifications.

Waivers of the Code

While some Company policies must be strictly adhered to, in other cases, exceptions may be possible. If you believe that a waiver of any of the principles or policies articulated in this Code is appropriate in a particular case, you should contact your manager first. If your manager agrees that a waiver is appropriate, the approval of the Legal Department must be sought and obtained.

Periodic Employee Certifications

Periodically, all Bitsight employees and directors are required to certify that they have reviewed this Code, understand it, and agree to be bound by its terms.

No Rights Created

This Code is a statement of the fundamental principles and certain key policies that govern the conduct of the Company's business. It is not intended to and does not create any obligations to or rights in any employee, director, customer, supplier, competitor, shareholder, or any other person or entity.

Where to Seek Help and Report Concerns

Reporting Concerns

Unless otherwise provided in this Code, reports of suspected violations of law, regulation, this Code or other Bitsight policies should be made to the Legal Department, the HR Department,

or through Bitsight's Anonymous Reporting Hotline through Lighthouse, as described below. When reporting potential violations, you should provide as much detailed information as possible, including the background and history of the potential violation, names, dates and places, and the nature of the potential violation.

Anonymous Reporting Hotline (Through Lighthouse)

Bitsight's Anonymous Reporting Hotline, which is administered by Lighthouse, is available to all Bitsight employees worldwide, and is open 24 hours a day, seven days a week, 365 days a year. The Anonymous Reporting Hotline offers services in all of the languages spoken in each country in which Bitsight has offices or employees.

How do I reach the Anonymous Reporting Hotline?

- **Via The Internet:** www.lighthouse-services.com/bitsight
- **By Telephone from Within the United States:** Dial (800) 603-2869
- **By Telephone from Outside of the United States:**

  Enter the AT&T Direct Dial Access® Code for your location (available at https://www.business.att.com/collateral/dial-guide.html). Then, at the prompt, dial (800) 603-2869.
- **By Email:** reports@lighthouse-services.com (must include company name with report)
- **By Fax From Within the United States:** (215) 689-3885 (must include company name with report)

Non-Retaliation Policy

Bitsight supports the right of each employee to report in good faith potential or suspected violations of applicable laws or regulations, the Code or other Bitsight policies or to provide information in connection with such report or complaint.
Retaliation against any employee for engaging in such activities will not be tolerated by Bitsight. Retaliation may take many forms and includes any adverse employment action against any individual who files a complaint in good faith or who participates in an investigation. Retaliation can also include actions intended to discourage a Bitsight employee from making or supporting a complaint.

Any Bitsight employee found to have retaliated against an individual for reporting in good faith a suspected violation of applicable laws or regulations, the Code, or other Bitsight policies, or for participating in an investigation of allegations of such conduct, will be subject to disciplinary action, up to and including termination of employment.