
Code of
Conduct
SI Group

Own Your Actions

Every day, our employees strive to innovate and drive change to create value with a passion for safety, chemistry, sustainability and extraordinary results. This is our purpose; each one of us is responsible for empowering and inspiring those around us. It is a choice we make to lead with integrity, take accountability, and create value.

Our Code of Conduct enables us to own our actions with confidence, knowing we always Do The Right Thing. We conduct our business in an honest and ethical way and will not seek unfair advantage through anticompetitive practices, fraud or the misuse of confidential information. While the Code cannot anticipate every issue that may arise, it provides a consistent framework to engage in ethical business practices as we navigate through a complex and evolving global environment.

The Code also offers guidance on how to raise questions and report potential misconduct. We rely on our employees, business partners and customers to use good business judgment and speak up with concerns.

Compliance is a critical part of our business. By following this Code and raising concerns, you are owning your actions. You are helping to foster a culture where we work well together and strengthen our company's integrity, reputation and future. Choose to own your actions and demonstrate your commitment to making a difference for SI Group, our environment and our global community.

Sincerely,
David Bradley
President and Chief Executive Officer

Table of Contents

Do the Right Thing

Our Values are a collection of seven bold statements centered around teamwork that guide our behaviors and interactions: Do the Right Thing; Captivate Our Customers; Results Matter; Lean In; Reach Beyond Your Possible; Better Every Day; and Embrace the Grit. In every decision we make and every action we take, we expect our employees, directors and officers to Do the Right Thing.

Employee Duty to Report Misconduct

SI Group has an open-door policy which means that we want all employees to feel comfortable asking questions or reporting concerns. Employees must be sensitive to situations that could result in a violation of law, regulation or this Code. Subject to certain data protection laws, employees have a duty to report any instance where they suspect misconduct by contacting one of the following:

- Any Compliance or Legal team member or email **compliance@siigroup.com**
- Any HR team member or email **hr@siigroup.com**
- SI Group's Hotline where reports can be made anonymously **www.siigroup.com/LivingOurValues**

Hotline

Any person can submit a misconduct report through our dedicated website or by calling an independent specialist at any time by visiting **www.siigroup.com/LivingOurValues**. The Hotline will provide an identification number to each person making a report, helping SI Group follow up with any anonymous reports and allowing the person making the report to obtain status updates. The Hotline will send all reports to SI Group for review. All reports will be taken seriously, kept confidential to the extent possible and addressed appropriately.

Compliance with Applicable Laws

SI Group is a global performance additives company operating in an industry with laws and regulations designed to protect our employees, customers, communities and the environment. It is our duty to comply with all laws and regulations that apply to our business. We will not tolerate unethical or illegal business practices by anyone doing business on our behalf. Actions on behalf of SI Group that violates law, regulation or this Code could lead to jail time, fines, lawsuits and termination of employment.

Retaliation

Retaliation is prohibited at SI Group. Retaliation occurs when an employer treats an employee or person associated with the business less favorably than others for engaging in certain protected activity, including but not limited to:

- Reporting a suspected violation or concern in good faith
- Participating in an investigation into a suspected violation or concern
- Opposing discrimination or other illegal behavior

SI Group respects the right of each employee to engage in protected activity. We rely on our employees to speak up so we can learn about issues and address them—after all, we make it a duty to report suspected violations of law, regulation and this Code because we value doing the right thing. We want all employees to feel comfortable raising concerns without fear of retaliation. Any employee who feels they are being threatened or discouraged from reporting a suspected violation or believes they are being retaliated against for reporting a suspected violation should contact HR, Compliance, Legal or the Hotline immediately. If SI Group concludes that an employee retaliated against a person for engaging in protected activity, the employee will face appropriate disciplinary action up to and including termination.

Our People

To succeed, our employees need work environments that promote confidence, inclusivity, and self-worth. The creation of these environments starts with you.

Diversity, Equity and Inclusion

SI Group's employees are our most valuable assets and we are passionate about nurturing a unique culture where employees enjoy coming to work every day. The fundamental benefit in promoting a diverse and inclusive global workforce is thought diversity. Our employees create value through differential performance, including their perspective, background and talent. Our goal is to foster an environment where employees feel valued and empowered to participate and contribute irrespective of their personal attributes.

Discrimination

SI Group is an equal opportunity employer and prohibits discrimination. Discrimination is treating a person unjustly based on a protected characteristic, including but not limited to age, race, color, sex, gender, gender identity, sexual orientation, marital status, national origin, citizenship, ancestry, religion, pregnancy, disability, or military or veteran status.

Equal opportunity and non-discrimination policies apply to all employment decisions at SI Group including recruiting, hiring, onboarding and training, job rotations, promotions, compensation, disciplinary actions and terminations.

In recognizing and respecting human rights, SI Group also complies with all applicable labor and employment laws including those relating to freedom of association and collective bargaining, competitive compensation and reasonable working hours, and the prohibition of child labor, forced labor and human trafficking.

We are committed to sustaining an inclusive culture, built upon our collective knowledge and respect for each other.

Privacy

Personal Data

To manage employment relationships and perform processes related to legitimate business interests, SI Group collects and uses personal data. We respect privacy and strive to protect the personal data of employees, customers and business partners in accordance with applicable laws, including the General Data Protection Regulation (GDPR), and contractual obligations. SI Group limits disclosure of sensitive personal data to only internal or external parties who need to know the information. We also use technology to help prevent unauthorized disclosures.

Recordings

To maintain personal privacy, prevent workplace harassment and protect confidential information, SI Group prohibits employees from making unauthorized or secretive audio, video or photographic recordings. Additionally, such recordings may violate local laws, which often require permission from any party being recorded.

Nepotism

SI Group seeks to minimize the conflicts of interest and discrimination that can occur when close relations work together. Subject to applicable laws, employees must disclose their family members and certain other close relations who work for SI Group as those relationships may present a conflict. Close relations must generally avoid working in the same team, sharing a manager, having a reporting relationship, and overseeing certain processes, compensation or disciplinary decisions relating to each other.

Harassment

Employees deserve a safe and welcoming environment to perform their work and create value. SI Group is committed to ensuring our employees work in an environment free from harassment. We do not tolerate harassment involving any of our employees, business partners or customers.

What is harassment?

Harassment is conduct that demeans, humiliates or embarrasses a person. There are different types of harassment including sexual harassment, discriminatory harassment, and in some jurisdictions, moral or power harassment. Sexual harassment includes unwelcome sexual conduct and conduct directed to a person because of their sex. Discriminatory harassment includes conduct that shows hostility or aversion toward protected characteristics such as age, race or religion. Moral and power harassment include bullying and abusive conduct such as yelling or criticism.

What are some examples of conduct that can constitute harassment?

- Verbal conduct such as derogatory jokes or comments, slurs, unwanted sexual advances, nicknames
- Visual conduct such as offensive or sexual posters, gestures, pictures, cartoons
- Written conduct such as offensive or sexual emails, texts, social media posts, handwritten notes
- Physical conduct such as unwanted touching, grabbing, hitting, cornering or blocking movement, interfering with work
- Threatening or demanding conduct such as forcing a person to take inappropriate action or provide a sexual favor, especially in the context of making employment decisions
- Retaliatory conduct against a person who made a good faith report or otherwise engaged in protected activity
- Any other conduct that creates a hostile work environment

Conduct can be perceived differently by reasonable people—what might not bother one person may make another person feel harassed or uncomfortable regardless of intent. SI Group employees, business partners and customers should always act professionally and respectfully when engaging with each other.

Where can harassment occur?

Harassment can occur anywhere, not just in the workplace. It can occur outside of the office or manufacturing site—during a commute; at an external meeting, afterwork happy hour or volunteer event; over video conference or voice calls; or through personal social media. When using any form of social media, remember that any harassment, bullying, discrimination or retaliation that would not be permissible in the workplace is not permissible online.

Any SI Group employee that is aware of potential harassment must report the conduct to HR, Compliance, Legal or the Hotline.

Health and Safety

Protecting and promoting the health, safety and well-being of SI Group employees is a top priority. To prevent work-related injury and achieve our goal of zero safety incidents, we have developed procedures to safely operate equipment, properly handle materials and limit exposure to potentially hazardous substances, among other safe work practices. To prevent illness, we have established global wellness protocols and we expect our employees to take reasonable care to further these efforts.

Own Your Actions

- Everyone at SI Group has the authority to intervene if they see something potentially dangerous occurring and can do so in a safe manner
- Report incidents to a manager, Environmental, Health and Safety (EHS) employee or Site Director in a timely manner so SI Group can properly respond to dangerous situations
- Do not skip quality checks
- Follow all rules regarding cell phone use, which can pose serious safety concerns throughout our sites
- Contact the global EHS team with questions or concerns

Cardinal Safety Rules

SI Group has implemented cardinal (lifesaving) safety rules that we deem critical to ensuring our employees are safe and protected from serious or fatal injuries. Employees must follow these rules, which relate to confined space entry, lock-out/tag-out, hot work permit, elevated work, overriding safety interlocks, enforcing cardinal safety rules and reporting potential violations of cardinal safety rules. More information is available in SI Group's Corporate EHS Cardinal Safety Rules **Policy**.

Substance Abuse

Employees, contractors and business partners must not perform any work on behalf of SI Group while under the influence of substances that impair judgment and ability to work safely and effectively. Such substances include alcohol, marijuana, illegal drugs and controlled substances like certain prescription medications. SI Group also prohibits illegal drug possession and related activities on company time and property.

SI Group will conduct drug and alcohol testing as permitted by local law to protect the safety of our employees.

Employees must report any suspected substance violations to HR, Compliance, Legal or the Hotline. Any employee who would like confidential assistance dealing with substance abuse or addiction should contact HR for information on professional resources.

Workplace Violence

As part of our commitment to a safe and comfortable work environment, SI Group does not tolerate workplace violence or threats. Like harassment, this prohibition encompasses all people engaged in SI Group business and can occur anywhere.

Examples of workplace violence include:

- Acting aggressively toward a person
- Physically harming a person
- Intentional destruction of SI Group or employee property
- Harassing or intimidating communication
- Stalking or secretive surveillance
- Bringing weapons to work
- Intentionally disregarding the safety and well-being of a person
- Threatening to do anything listed above

Employees must report suspected workplace violence and threats to HR, Compliance, Legal or the Hotline.

Our Business

Achievements are earned, and so is respect. Always remember that the way you conduct business is vital to our company accomplishing both.

Bribery and Corruption

SI Group employees are encouraged to develop strong relationships with customers and business partners, and we recognize that gifts and business courtesies may be part of legitimate business activity.

Gifts and business courtesies are generally allowed when they are:

- Given without corrupt intent
- Reasonable and modest in value
- Provided openly and transparently
- In compliance with local law, local custom and this Code

SI Group does not tolerate corruption by any employee or business partner acting on our behalf. Anti-bribery and corruption laws prohibit giving anything of value to public officials with the intent to influence their decisions and obtain a business advantage. This includes giving cash, gifts, business courtesies (such as travel, entertainment or dining), facilitation payments, and charitable or political donations. Likewise, employees and business partners are prohibited from receiving anything of value as a personal incentive to conduct business on SI Group's behalf. While laws focus on public officials' involvement in corrupt schemes because of the influence they can exert, SI Group also prohibits employees and business partners from engaging in corrupt conduct involving private parties.

Corruption is often newsworthy and can result in financial and reputational risk. To ensure compliance with anti-bribery and corruption laws, SI Group has approval and disclosure requirements on gifts and business courtesies. We also perform due diligence and monitoring on business partners that are likely to engage with public officials. More information is available in SI Group's Anti-Bribery and Corruption **Policy and Procedure**.

Own Your Actions

- Know our business partners – if something seems suspicious, contact Compliance immediately
- Do not offer or accept bribes or kickbacks
- Always get a receipt and keep accurate books and records
- Contact Compliance with questions or concerns

International Trade

International trade laws help prevent corruption, terrorism, trafficking, weapons proliferation and other dangerous crimes by restricting certain business transactions and cross-border trade. With offices, manufacturing sites, distributors and customers across the globe, SI Group must comply with all applicable international trade laws. These laws vary across the globe and sometimes conflict with each other. Our global Regulatory team, in addition to Compliance, can provide guidance and expertise in the area.

Sanctions

Trade sanctions prohibit or restrict trade with certain persons and entities (watchlists), countries (embargoes) and industries (sectoral sanctions). SI Group cannot engage in certain prohibited dealings with sanctioned parties or certain parties whose beneficial owners are sanctioned.

Controls

Trade control laws restrict the export of certain goods, services, software and technology and require licenses for certain exports. The laws restrict business travel and sharing information with certain countries or people (including by transporting a laptop). The laws also dictate import requirements relating to classification, country of origin, and value of goods, services, software and technology.

Boycotts

Many countries have laws requiring companies to refuse to do business with a particular country (a boycott). Countries' boycott laws often conflict with each other.

Antitrust and Competition

Antitrust and competition laws are designed to protect our customers and ensure entrepreneurship can flourish. Conducting business meant to unreasonably restrain trade or abuse a dominant market position is generally illegal. SI Group strives to have popular products and strong sales by offering exceptional value, quality and service. It is our policy to compete vigorously and fairly, exercise independent judgment in running our business and comply with all antitrust and competition laws. Antitrust and competition laws are complicated, fact-dependent and vary across the globe. More information is available in SI Group's Antitrust **Policy and Procedure**.

Contact with Competitors

Agreements between competitors that are designed to limit competition are the most common and serious antitrust law violations. Employees must:

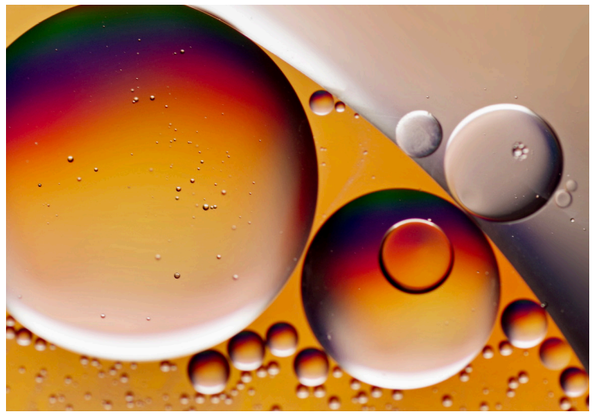
- Avoid any action that harms competition
- Avoid discussing competitively sensitive information with competitors including prices, costs, profits, product or service offerings, credit policies, proprietary processes, terms or conditions of sales, deliveries or sales volumes, production capacities or volumes, market share, decisions to quote, common customers or suppliers, sales territories, distribution or channel strategies, or marketing or promotional strategies
- Obtain pre-approval from Compliance if a procompetitive business purpose arises where certain competitively sensitive information needs to be shared with a competitor to complete a deal
- Limit conversations with customers who are competitors downstream to general information on the amount and type of product the customer would like to buy and the price SI Group is offering for the product
- Document and report certain competitor contacts

Trade and Industry Associations

Trade and industry associations provide procompetitive and educational opportunities to learn more about our industry, obtain information that enables sellers and customers to make informed decisions, and engage in standard setting functions and lobbying activities. Since SI Group competitors often join these associations and attend events, employees must comply with approval and reporting requirements related to association activities.

Own Your Actions

- Use independent judgment when making business decisions about what products to sell and where to sell them
- Obtain market intelligence from public sources or customers who volunteer information – not competitors
- Make pricing decisions based on SI Group costs, general market conditions and public information
- Make factual statements about SI Group's products and why they may be superior to competitors' products
- Allow customers to purchase one or many products offered by SI Group – do not require customers to purchase products as a bundle
- Contact Compliance with questions or concerns



Conflicts of Interest

Employees have a duty to conduct SI Group business dealings in the best interest of our company. Doing so helps maintain our reputation, credibility, independence and compliance with applicable laws. A conflict of interest exists where an employee's personal interests interfere with, or have the potential to interfere with, the interests of SI Group. Conflicts may arise from outside employment or financial interests in any entity but may be most likely to arise from interests in business partners, customers and competitors. Employees must disclose outside interests and work with SI Group to eliminate any actual or potential conflict of interest. Employees must never use SI Group resources to advance personal interests. More information is available in SI Group's Conflicts of Interest **Policy and Procedure**.

What can create a conflict of interest?

- Second jobs or affiliations, whether paid or unpaid
- Board memberships
- Interacting with close relations while conducting SI Group business
- Close relations who are public officials or have decision-making authority for business partners, customers or competitors
- Financial interests or investments
- Romantic or family relationships between employees when one employee can influence the other's job responsibilities, salary, performance rating or promotion

How can conflicts harm SI Group?

- Insufficient time to complete SI Group work due to competing work priorities
- SI Group resources or technology misused for non-SI Group purposes
- Implication that SI Group supports or sponsors an entity or organization
- Appearance of corruption (gifts to or from a public official)
- Appearance of anticompetitive behavior (obtaining business in an unfair way)

Technology and Cybersecurity

SI Group technology resources such as laptops, cell phones and internet are critical to our business, and employees have a duty to protect these and all business resources from damage, theft and misuse. SI Group tech resources must never be used to advance personal interests or for illegal or inappropriate activities such as streaming, downloading or sharing pornography or material that is discriminatory or otherwise offensive. Subject to applicable law, employees have no reasonable expectation of privacy while using SI Group technology resources and SI Group reserves the right to monitor individual technology use and system activity.

Cybersecurity Practices

Cybersecurity is the responsibility of all employees, not just IT. Regardless of whether employees use company or personal tech devices to conduct business, employees must:

- Secure devices in a safe location – if a tech device is lost, stolen, or accessed by an unauthorized user, contact IT immediately
- Password protect tech devices with complex passwords in accordance with the Strong Password Policy
- Never share usernames or passwords with anyone
- Never attempt to circumvent any IT controls, which are in place to protect SI Group's network and maintain proper business processes
- Only use software licensed by SI Group – downloading or using unlicensed software to conduct SI Group business is prohibited
- Never create or copy an SI Group file containing confidential information on any tech device or software not authorized by SI Group
- Only conduct SI Group business through authorized communication channels made available by IT such as Outlook email – using unauthorized, unprotected communication tools such as WhatsApp, WeChat or social media platforms to conduct business is prohibited
- Watch out for any phishing attempts and do not connect any unauthorized devices to SI Group's tech devices
- Complete all required IT training and implement all recommended practices
- Report suspicious behavior or unauthorized activity to IT as soon as possible

Intellectual Property

Intellectual property (IP) is one of our most valuable assets at SI Group. While not a physical asset, IP is information-based and encompasses the formulas and production methods used to manufacture our proprietary additives and resins. IP includes patents (rights to an invention), trademarks (identifying brands or services), copyrights (such as text on a website or in marketing literature), and trade secrets (such as formulas and process conditions).

SI Group employees must take appropriate steps to establish, safeguard, and maintain IP assets while always respecting the IP rights of others. Employees must never use our IP to advance personal interests.

Protecting Our IP

An invention is any new, nonobvious and useful work, such as a composition, process, method, or device. Patented inventions can provide SI Group with a distinct competitive advantage. Employees must effectively identify and record such IP using available SI Group systems shortly after development to avoid the inadvertent loss of rights and allow for the maximum available protection under law. The Legal team can provide additional guidance and expertise in this area.

Question: I have developed a new formula for an antioxidant additive for SI Group. To evaluate effectiveness and performance, my strategic business unit sold an experimental sample to a customer. A non-disclosure agreement was not in place. Does this present a problem for SI Group?

Answer: Yes. Intellectual property laws in many key markets prevent SI Group from filing a patent application after making a public disclosure. The sale of the sample is a public disclosure. Not having a non-disclosure agreement in place with the customer during the sale is also a public disclosure. Even giving a free sample to a customer without a non-disclosure agreement in place is a public disclosure. Without patent protection, SI Group competitors can use the formula without fear of legal consequences. To evaluate a sample's effectiveness and performance while protecting SI Group's new product development, we require a non-disclosure agreement to be in place with the customer and then give them a free sample to test.

Respecting Others' IP

Just as we expect third parties to respect our IP rights, we must respect their IP rights. We cannot use others' IP without fairly compensating the IP owner.

Question: An employee is preparing a presentation that will be seen by external parties, such as customers and suppliers. The employee found photographs on the internet that would help illustrate points in the presentation. Can the employee use these photographs in the presentation?

Answer: Maybe, but contact our Global Brand and Communications team before using any material found on the internet. In most cases, the employee would be advised to use a stock photo that SI Group has purchased the right to use. Also, some material on the internet may not have IP protection and may be freely available for public use. Other material may be protected by copyright even if a copyright notice is not included with the material.

Question: A new employee who used to work for an SI Group customer offered to share information on their former employer's new product development strategy. The information would be very useful to SI Group's product development strategy. Can the employee share this information with the team?

Answer: Usually no, and always contact Legal before sharing this information. The former employer's product development strategy is most likely a trade secret that has not been made public. The new employee may also have a non-disclosure agreement in place with the former employer and sharing the trade secret would violate the agreement. The value SI Group could gain in knowing the information would likely not outweigh the potential IP and reputational risks that could stem from receiving the information.

Confidential Information

SI Group employees have a duty to protect confidential information to help SI Group comply with legal requirements and encourage customers' and business partners' good faith disclosures. Confidential information is non-public information about our internal business practices and products, our customers and business partners, and our employees. Proprietary information, personal data and material non-public information are all categories of confidential information.

Sharing Confidential Information

Confidential information should only be shared with employees or third parties who have a business need to know, meaning they require the information to perform a valid job function. Legal must approve a non-disclosure agreement before disclosing confidential information to a third party.

Employees must continue to protect confidential information after employment ends (and similarly, employees must not disclose confidential information belonging to a previous employer).

Own Your Actions

- Do not discuss confidential information with anyone who does not have a business need to know (including family and friends)
- Be proactive to prevent unintentional disclosures – ensure tech device screens are not visible and do not discuss confidential information in a public setting (public transit, hotels, restaurants, sporting events)
- Do not post or discuss confidential information on social media, unauthorized instant messaging platforms or unprotected networks
- Do not use personal email accounts or unauthorized services outside of SI Group's network to share or store confidential information
- Securely store confidential information – password protect sensitive data files and share the files and passwords in separate emails
- Contact Compliance with questions or concerns

Definitions

Proprietary Information

Information that SI Group developed, created or discovered and information conveyed to SI Group that has commercial value to our business. Examples of proprietary information include our intellectual property (patents, copyrights, trade secrets); ideas, techniques, formulas, inventions; non-public algorithms; business processes; customer lists; and terms and prices to customers.

Personal Data

Information that can be used to identify a person. Examples of personal data include name, age, email address, physical address, educational background. Sensitive personal data includes social security number, passport or driver's license information, compensation, bank account information, personnel files and performance information, medical information, biometric data, sexual orientation, race, religion and criminal history.

Material Non-Public Information

Information that could reasonably affect the market price of publicly traded securities or influence investor decisions on securities trading and has not been broadly disseminated to the market. Examples include sales results or estimates; strategic plans; new products; joint ventures, acquisitions or divestitures; proposed securities offerings; regulatory actions; government investigations; litigation; restructuring or senior management changes; and major contract negotiations.

Insider Trading

SI Group employees may have material non-public information about our business or our business partners. Material non-public information is also known as inside information or price-sensitive information. To comply with insider trading and securities laws, employees must not use or have a company's material non-public information when trading that company's securities. It is also possible for employees to violate these laws by disclosing material non-public information to another person who does not have a business need for the information, particularly if it motivates the person to trade using the information. Such a disclosure is known as tipping. It is possible to violate insider trading laws by tipping even if the employee who made the disclosure did not financially benefit from the disclosure or intend to engage in insider trading.

SI Group will comply with all applicable laws when making material non-public information disclosures about our business and will not make selective disclosures. Contact Compliance with any questions.

Accurate Business Records

Maintaining accurate and complete business records is vital to SI Group's business decisions and reporting obligations to investors, creditors, government agencies and others. We must:

- Prepare business records in accordance with law, SI Group policies and generally accepted accounting principles
- Ensure that underlying transactions are accurately and fairly reflected in the record and incorporate supporting documentation – never create fraudulent documents or misrepresent the details of transactions (e.g., indicate an earlier date for a transaction than when it occurred)
- Ensure that actions and commitments are in accordance with SI Group's Delegation of Authority
- Establish and maintain strong and effective internal controls
- Maintain and destroy records pursuant to law and SI Group's record retention policies

Fraud

Employees must not engage in fraud relating to SI Group business. Fraud is an untrue representation of facts designed to benefit the party engaged in fraud or deny a right to the party receiving the information (for example, a customer or government agency). Fraud includes providing a false statement, omitting relevant information or misrepresenting a situation. Employees must ensure information they document and approve is accurate and complete. Employees should be able to prove factual statements about our products and financial information.

Internal Controls

Employees, contractors and other business partners are prohibited from attempting to circumvent any SI Group internal controls. Such controls are designed to safeguard SI Group assets and ensure the accuracy, completeness and appropriate approval authority of SI Group processes and business records.

Our Social Responsibility

The many spaces we share extend outside SI Group's walls. By bringing our values with you, you help to create places we all want to be.

Environment and Sustainability

SI Group is dedicated to protecting the environment and respecting the communities where we operate and live. As a chemical company, we are aware of the risks and hazards we face every day and understand that developing sustainable practices with the future in mind is vital to our business continuity and success. As part of our commitment to the environment and sustainability, we:

- Commit to safety and compliance with all applicable environmental, health and safety laws
- Adhere to ethical and system standards
- Leverage natural resources efficiently to minimize the impact on the environment
- Evaluate our processes and performance to drive improvement
- Reduce risks associated with our products and dispose waste in a socially responsible manner
- Innovate to provide reliable products that solve customer challenges

Our EHS goals are zero impacts on safety, the environment and our brand. In addition, we practice product stewardship to protect customers and other stakeholders, anticipate and respond to new expectations, and minimize resource and energy use.

Suppliers

SI Group expects our suppliers and business partners to uphold these environmental and sustainability values and comply with environmental, conflicts minerals, labor and ethics laws in accordance with SI Group's **Supplier Code of Conduct**. We review our relationships with suppliers and business partners and terminate relationships that do not meet our expectations.

Reporting Incidents

SI Group strives to exceed minimum environmental law requirements to protect the environment and neighboring communities. In the event of an incident that may impact the environment, employees must contact Corporate EHS, which will initiate appropriate emergency response measures and communications. While we comply with applicable law and regulation, where local law is less stringent than SI Group policy, SI Group policy applies. More information is available in SI Group's Environmental Sustainability **Policy**.

Community Engagement

SI Group values the communities where we operate and live. We encourage our employees to be engaged citizens who participate in community events, volunteer with charitable organizations and fulfill civic duties. Additionally, SI Group may partner with local charities or make charitable contributions in accordance with the Antibribery and Corruption **Policy and Procedure**.

Political Activities and Contributions

SI Group encourages employees to participate in or donate to political processes, but such activities must be done independently by each employee outside of work hours with no implication that the activity is on behalf of SI Group. Employees must not use any SI Group resources (such as SI Group letterhead or email) when engaging in personal political activity. Local laws prohibit SI Group from making certain political contributions. Any proposed political contribution by SI Group must be pre-approved in accordance with the Antibribery and Corruption **Policy and Procedure**. Additionally, any employee participating in standard setting or legislative activities, such as lobbying, must be pre-approved in accordance with the Antitrust and Competition **Procedure**.

Transparency and Communication

Transparency is important at SI Group. We seek to communicate with our communities, customers, investors and other stakeholders about our business in an accurate, consistent and timely manner. Employees must not speak on behalf of SI Group unless it is their job to do so. To ensure our public messaging is aligned with our brand, Code and applicable law, all public messaging including press releases, social media posts and crisis communications must be approved by Global Brand and Communications. Any employee who becomes aware of any misuse of social media related to SI Group's business or brand must contact Global Brand and Communications.

Our Response to Misconduct

What happens after SI Group becomes aware of a concern or report of a suspected violation of law, regulation or this Code? Compliance, Legal or HR will review the matter, request necessary additional information and take appropriate action. Concerns or reports that would not result in a violation of law, regulation or this Code may be handled by HR or referred to management. Reported allegations that would lead to a violation of law, regulation or this Code if substantiated will be investigated in a fair, impartial and timely manner.

Investigation Process

SI Group's internal investigations will comply with local laws and be led by investigators with subject matter expertise (typically Compliance, Legal or HR). Investigations will be confidential to the extent possible, meaning the investigators will only share information on a need to know basis or as required by law. The names of any concern raisers that report suspected violations will not be disclosed to the employee(s) suspected of violations unless required by law.

Investigations vary based on the allegation, but generally include:

- Action to protect the concern raiser, if necessary
- Review of relevant policies, emails or other documents
- Interviews with relevant employees
- Recommended corrective action, including process changes, training or discipline
- A written report documenting findings

Employees have a duty to cooperate with investigations (and audits or other reviews), provide accurate and complete information, and never alter or destroy records related to an investigation or anticipated investigation. The employee that is the subject of the investigation may have the right under local law to access and correct information related to an investigation. Any employee who fails to cooperate with an investigation, or who retaliates against another employee for reporting a suspected violation in good faith or cooperating with an investigation, will be subject to disciplinary action up to and including termination.

Litigation and Government Investigations

SI Group may be involved in litigation or government investigations. Any employee who receives a request for information from a third party that relates to litigation or a government investigation must advise that they will cooperate with the request but needs to contact Legal before providing any information. Contact Legal for additional guidance on responding to requests for information.

Whistleblower Protection

This Code does not limit employee rights to provide truthful disclosures of confidential information to government or regulatory agencies under the whistleblower provisions of applicable law or regulation. SI Group prohibits retaliation against any employee for reporting in good faith any suspected wrongdoing or for cooperating with a government investigation.

Certifying to our Code

SI Group employees must periodically certify to this Code to confirm that they have reviewed it, understand it, and agree to comply with it. During the certification period employees must also disclose any previously unreported suspected violations subject to applicable law.

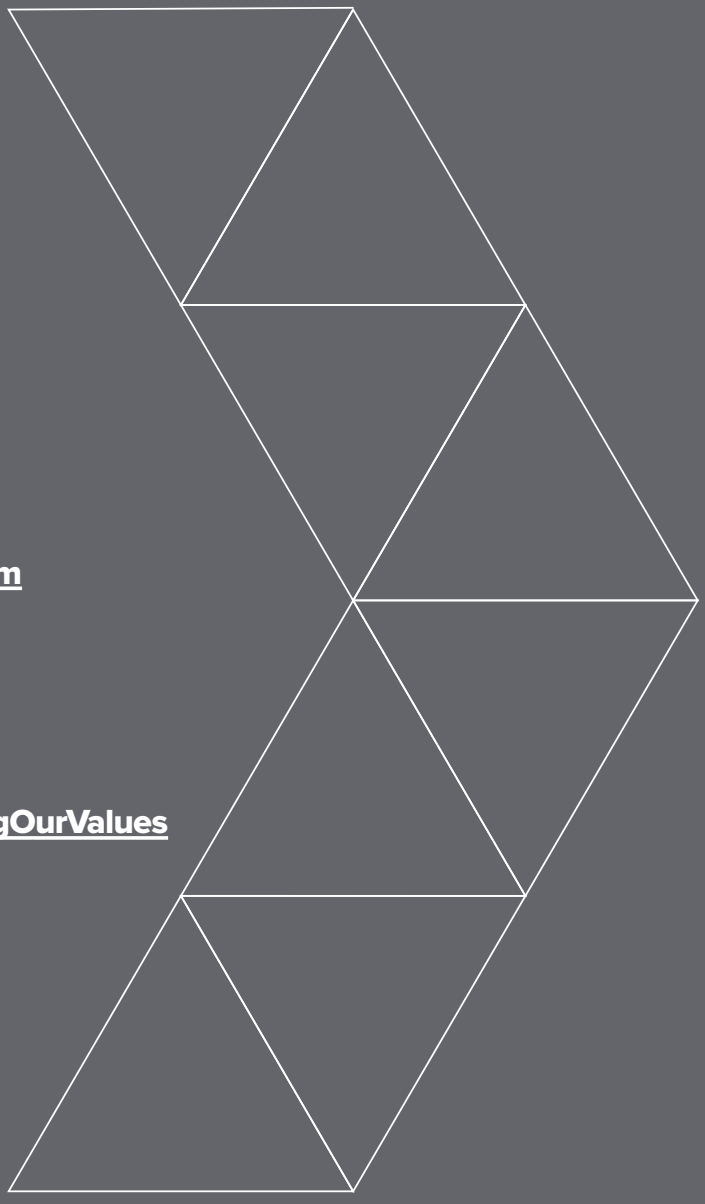
Own Your Actions

Contact Information

Compliance
compliance@siigroup.com

HR
hr@siigroup.com

Hotline
www.siigroup.com/LivingOurValues



SI Group