



Effective January 1, 2020

Revised September 1, 2025

EMERALD HOLDING, INC.

CODE OF BUSINESS CONDUCT AND ETHICS

Seeking Guidance and Information; Compliance	1
Conflicts of Interest.....	2
Corporate Opportunities	3
Gifts and Entertainment.....	3
Financial Information and Disclosure	4
Company Records.....	5
Confidentiality.....	5
Information Security Policy.....	6
Protection, Return, and Proper Use of Company Assets	6
Information Security Roles and Responsibilities.....	7
Fair Dealing and Competition	8
Compliance with Laws, Rules and Regulations.....	9
Information Security Risk Management.....	9
Interactions with the Government	9
The Foreign Corrupt Practices Act.....	10
Employment Practices.....	11
Remote Work.....	13
Address Change	14
Employee Privacy.....	14
Environmental, Health and Safety	14
Compliance with Antitrust Laws	14
Political and Charitable Activities	16
Insider Trading Laws	17
Public Communications and Fair Disclosure	17
Waivers.....	18
Consultation, Reporting and Retaliation.....	18
Consequences of Violation	18
Conclusion	19

EMERALD HOLDING, INC.

CODE OF BUSINESS CONDUCT AND ETHICS

This Code of Business Conduct and Ethics (this “Code”) contains general guidelines for conducting the business of Emerald Expositions Events, Inc. and its subsidiaries (collectively, the “Company”) consistent with the highest standards of business ethics. To the extent this Code requires a higher standard than required by commercial practice or applicable laws, rules or regulations, we adhere to these higher standards. This Code reflects our commitment to a culture of honesty, integrity and accountability and outlines the basic principles and policies with which all Company directors, officers, and employees (collectively, for purposes of this Code, “employees”) are expected to comply. Additionally, every independent contractor who acts for the Company is expected to read, understand, and acknowledge this Code and observe the same ethical standards of conduct as employees when conducting business with or for the Company. No person may indirectly, through any third party, do anything such person is prohibited from doing under this Code.

Failure to observe applicable laws or the ethical business standards contained in this Code may expose the Company and its employees to criminal indictment, legal sanctions, financial penalties, and/or a tarnished reputation. All of the Company’s employees are expected to be honest, objective and diligent in the performance of their duties and responsibilities. They are trusted by the Company to exhibit loyalty in all matters pertaining to the Company’s affairs and to not engage in any illegal or improper activity.

Seeking Guidance and Information; Compliance

This Code is not intended to be a comprehensive rulebook and cannot address every situation that you may face. Employees are expected to observe both the spirit and the letter of this Code and to consult this Code or an appropriate representative of the Company when faced with an ethical issue. If you feel uncomfortable about a situation or have any doubts about whether it is consistent with the Company’s ethical standards, seek guidance. We encourage you to contact your supervisor for help first. If your supervisor cannot answer your question or if you do not feel comfortable contacting your supervisor, contact the Company’s Chief Executive Officer, Chief Financial Officer, or General Counsel.

The Company has also established a Whistleblower Hotline that is staffed by an unaffiliated third party service provider and is available 24 hours a day, 7 days a week at 1-855-MRLDXPO (1-855-675-3976). You may remain anonymous and will not be required to reveal your identity in calls to the Whistleblower Hotline, although providing your identity may assist the Company in addressing your concerns. All reports of known or suspected violations of the law or this Code will be handled sensitively and with discretion. Your supervisor and Company management will protect your confidentiality to the extent possible, consistent with law and the Company’s need to investigate your concern.

The elements of this Code are in addition to other Company policies and employee training which, in some cases, may be more specific. These additional training tools are a part of the Company’s ongoing commitment to maintaining a culture of sound ethics and integrity.

It is the Company’s policy that no one will suffer any reprisal, retaliation or punishment for reporting, in good faith, incidents that might be in violation of law or this Code.

Conflicts of Interest

Each Company employee must avoid any conflict, or perception of conflict, between his or her personal interests and the interests of the Company in transacting Company business. A conflict situation can arise when an employee (a) has a personal interest that would be likely to interfere with or appear to interfere with the Company's interests or the employee's loyalty to, or judgment on behalf of, the Company, (b) chooses or may appear to have chosen a personal interest over the interests of the Company or (c) takes actions or has interests that may make it difficult or appear to make it difficult to perform his or her work objectively and effectively.

Identifying potential conflicts of interest may not always be clear-cut. Some examples of potential conflicts of interest include, but are not limited to:

- *Outside Employment.* No employee should be employed by, serve as a director of, or provide any services to a company that the individual knows or suspects is a material customer or supplier, or is a competitor, of the Company, or that has interests that reasonably would be expected to conflict with the interests of the Company, or where that relationship or competition with the Company is a material part of the other company's business. Additionally, employees should devote their full professional attention and time to the Company and their job duties during the time that they are required to be working for the Company. If the Company determines that an employee's outside work or activities interfere with his or her performance, the employee may be required to terminate the outside employment or activity if he or she wishes to remain employed by the Company.
- *Improper Personal Benefits.* No employee should obtain any material (as to him or her) personal benefits or favors because of his or her position with the Company. Please see "Gifts and Entertainment."
- *Financial Interests.* No employee should have a significant financial interest (ownership or otherwise) in any company that the individual knows or suspects is a material customer or supplier, or is a competitor, of the Company, or where that relationship or competition with the Company is a material part of the other company's business. A "significant financial interest" means (i) ownership of greater than 1% of the equity of a material customer or supplier, or competitor or (ii) an investment in a material customer or supplier, or competitor that represents more than 5% of the employee's net worth.
- *Loans or Other Financial Transactions.* No employee should obtain loans or guarantees of personal obligations from, or enter into any other personal financial transaction with, any company that the individual knows or suspects is a material customer or supplier, or is a competitor, of the Company, or where that relationship or competition with the Company is a material part of the other company's business. This, however, does not prohibit arms-length transactions with banks, brokerage firms or other financial institutions.
- *Actions of Family Members.* The actions of family members outside the workplace may also give rise to the conflicts of interest described above because they may influence an employee's objectivity in making decisions on behalf of the Company. For purposes of this Code, "family members" include your spouse or life-partner, brothers, sisters and parents, in-laws and children whether such relationships are by blood or adoption, as well as anyone else residing in your household.

For purposes of this Code, the Company's Chief Financial Officer or General Counsel may determine, in his or her discretion, whether a company is a "material" customer or supplier of the Company. If you are uncertain whether a particular company is a material customer or supplier, please contact the Company's General Counsel for assistance.

The Company requires that employees disclose any situation that reasonably would be expected to give rise to a conflict of interest. If you suspect that you have a conflict of interest, or something that others could reasonably perceive as a conflict of interest, you must report it in writing to your supervisor or the Company's Chief Executive Officer, Chief Financial Officer or General Counsel. Such person will work with you to determine whether you have a conflict of interest and, if so, how best to address it. Although conflicts of interest are not automatically prohibited, they are not desirable and may only be waived as described herein under "Waivers".

Corporate Opportunities

As an employee of the Company, you have an obligation to advance the Company's interests when the opportunity to do so arises. If you discover or are presented with a business opportunity through the use of corporate property or information or because of your position with the Company, you should first present the business opportunity to the Company before pursuing the opportunity in your individual capacity. No employee may use corporate property, information or his or her position with the Company for personal gain, nor compete with the Company while employed by the Company.

You should disclose to your supervisor the terms and conditions of each business opportunity covered by this Code that you wish to pursue. Your supervisor will contact the Chief Financial Officer to determine whether the Company wishes to pursue the business opportunity. If the Company waives its right to pursue the business opportunity, you may pursue the business opportunity on the same terms and conditions as originally proposed and consistent with the other ethical guidelines set forth in this Code.

Gifts and Entertainment

The giving and receiving of small gifts is often a common business practice. Appropriate business gifts and entertainment are welcome courtesies designed to build relationships and understanding among business partners. Gifts and entertainment, however, should not compromise, or appear to compromise, your ability to make objective and fair business decisions.

It is your responsibility to use good judgment in this area. As a general rule, you may give or receive gifts or entertainment of nominal value to or from customers or suppliers only if the gift or entertainment would not be viewed as an inducement to or reward for any particular business decision. All gifts and entertainment expenses must be properly accounted for on expense reports.

No gift may be offered or accepted if it will create a feeling of obligation, compromises judgment, appears to improperly influence the recipient, or acts as an inducement for an action that is illegal, unethical, a breach of trust or the improper performance of a function or activity. In no event may any employee accept any cash gifts, gift cards, or gifts of securities from anyone with whom the employee has a business relationship.

The following specific examples may be helpful:

Meals and Entertainment. You may occasionally accept or give meals, refreshments or other entertainment if the items are of reasonable value, a primary purpose of the meeting or attendance at the event is business related, and the expenses would be paid by the Company as a reasonable business expense if not paid for by another party. Entertainment of reasonable value may include food and tickets for sporting and cultural events if they are generally offered to other customers, suppliers or vendors. Accepting normal business entertainment, at which the giver is present, such as lunch, dinner, theater, a sporting event or other customary business entertainment, is appropriate if of a reasonable nature and in the course of a meeting or to foster better business relations.

Personal Gifts. With respect to business associates, you may accept or give personal gifts of reasonable value (generally under \$50) that are related to recognized special occasions such as a graduation, promotion, new job, wedding, retirement or holiday.

Gifts Rewarding Service or Accomplishment. You may accept a gift from a trade association or a civic, charitable or religious organization specifically related to your service or accomplishment.

If you conduct business in other countries, you must be particularly careful that gifts and entertainment are not construed as bribes, kickbacks or other improper payments. See “The Foreign Corrupt Practices Act” for a more detailed discussion of the Company’s policies regarding giving or receiving gifts related to business transactions in other countries.

You should make every effort to refuse or return a gift that is beyond these permissible guidelines. If it would be inappropriate to refuse a gift or you are unable to return a gift, you should promptly report the gift to your supervisor. Your supervisor will bring the gift to the attention of the Chief Financial Officer or General Counsel, who may require you to donate the gift to an appropriate community organization. If you have any questions about whether it is permissible to accept a gift or something else of value, contact your supervisor or the Chief Financial Officer or General Counsel for guidance.

Gifts and entertainment may not be offered or exchanged under any circumstances to or with any employees of the U.S., state or local governments or of foreign governments. For a more detailed discussion of special considerations applicable to dealing with the U.S., state and local governments, see “Interactions with the Government.” For a more detailed discussion of special considerations applicable to dealing with foreign governments, see the Company’s FCPA and Anti-Bribery Policy.

Financial Information and Disclosure

The Company requires fair, timely, full and accurate recording and reporting of financial information in order to make responsible business decisions and appropriate disclosures under applicable securities laws. Within their areas of responsibility, employees are responsible for making sure that the Company’s financial statements, records, accounts, and supporting documents: (a) accurately and fairly reflect, in reasonable detail, the assets and transactions of the Company and comply with applicable legal and accounting requirements and reporting procedures; (b) are safeguarded from loss or destruction; (c) are retained for specified periods of time in accordance with the Company’s document retention policy; and (d) are maintained in

confidence. In order to achieve this, each employee must be familiar with his or her responsibilities in connection with the disclosure requirements generally applicable to the Company.

No employee should knowingly misrepresent, or knowingly cause others to misrepresent, facts about the Company to others, whether within or outside the Company or to governmental regulators and self-regulatory organizations. Employees must not forge, falsify or omit important facts to mislead others in any documents or in any communications. All Company accounting records, financial reports and supporting documents must be kept and presented in accordance with the standards and laws of each applicable jurisdiction and generally accepted accounting standards, and must accurately and fairly reflect the Company's assets, liabilities, revenue and expenses. Employees must not engage in any conduct calculated or likely to inhibit management, internal audit, external audit, or the legal or finance functions from achieving a proper understanding of relevant aspects of the business and the risks associated therewith.

In connection with its public communications as a public company, the Company is required to comply with a rule under the federal securities laws referred to as Regulation FD (which stands for "fair disclosure"). Regulation FD mandates that public companies avoid selectively disclosing market-sensitive information to participants in the securities markets. "Securities market professionals" generally include broker-dealers, analysts, investment advisors, institutional investment managers, mutual funds, hedge funds and similar entities. Please read carefully and comply with the Company's Disclosure Policy.

When litigation or a governmental investigation or audit is pending or imminent, relevant records must not be altered or destroyed. Destruction of records to avoid disclosure in a legal or governmental proceeding or in an internal investigation is a violation of this Code and may also be a criminal offense. Do not dispose of documents if the documents are subject to legal preservation requirements. When in doubt, always err on the side of retention.

Company Records

Accurate and reliable records are crucial to our business. Our records are the basis of our earnings statements, financial reports and many other aspects of our business and guide our business decision-making and strategic planning. Company records include financial records, personnel records, including expense reports, and all other records maintained in the ordinary course of our business. All Company records must be complete, accurate and reliable in all material respects.

Confidentiality

In carrying out the Company's business, employees often have access to confidential or proprietary information about the Company, its investors and business partners, or other third parties. Employees must protect the confidentiality of such information, except when disclosure is authorized or legally mandated. Confidential information includes, among other things, any non-public information concerning the Company, including its businesses, financial performance, results or prospects, financial and other information about potential acquisitions and any non-public information provided by a third party with the expectation that the information will be kept confidential and used solely for the business purpose for which it was conveyed. All information regarding the business, affairs and activities of the Company should be considered confidential by employees unless and until it is properly made available to the public. Any

employee who receives confidential information is prohibited from disclosing such information to any other person unless it is necessary to do so in the conduct of the Company's business and then only if the employee takes appropriate steps to protect the continuing confidentiality of such information.

In order to prevent the misuse or inadvertent disclosure of material information, the procedures set forth below should be observed at all times:

- confidential matters should not be discussed in places where the discussion may be overheard, such as elevators, restaurants, or airplanes;
- confidential documents should not be read in public places, left in unattended conference rooms, left behind when a meeting is over or discarded where they can be retrieved by others;
- care should be taken in communicating confidential matters on wireless devices;
- transmission of confidential information via electronic means, such as by fax or e-mail, should be made only where it is reasonable to believe that the transmission can be made and received under secure conditions;
- access to confidential electronic data should be restricted through the use of passwords;
- unnecessary copying of confidential documents should be avoided and extra copies of confidential documents should be shredded or otherwise destroyed;
- documents and files containing confidential information should be kept in safe and controlled locations;
- all proprietary information, including computer programs, analyses, models and other records, are the property of the Company and may not be removed, disclosed, copied or otherwise used except in the normal course of employment or with prior authorization.

When leaving the Company, an employee must return all confidential information in his or her possession and is required to continue to protect any confidential information learned during the course of his or her employment.

Information Security Policy

Emerald is committed to protecting the confidentiality, integrity, and availability of its information assets in accordance with international standards, including ISO 27001. All employees, contractors, and third parties must comply with the organization's information security policies and procedures. Information security is essential to maintaining trust with our customers, partners, and stakeholders, and to ensuring the continued success of our business operations.

Protection, Return, and Proper Use of Company Assets

The Company purchases goods and services, including business supplies, computer and communication equipment and software, for its business purposes. Employees may not direct the Company's money, supplies, materials or other property or resources, for personal use. Furthermore, it is the employee's responsibility to ensure that any Company property issued to him or her is kept in good condition and properly maintained.

Upon termination of employment or at the company's request, employees are required to promptly return all company property, including laptops, mobile devices, access cards, documents, and any other materials or equipment issued during their employment. Failure to return company property may result in the withholding of final paychecks, legal action, or other disciplinary measures. Employees are expected to ensure that all returned items are in good condition, and any loss or damage should be reported immediately to the Human Resources department.

Employees should protect the Company's assets and ensure their efficient use for legitimate business purposes only. Theft, carelessness and waste have a direct impact on the Company's profitability. The use of Company funds or assets, whether or not for personal gain, for any unlawful or improper purpose is prohibited. None of the Company's assets, funds, facilities, personnel or other resources should be used for personal purposes unless authorized under a separate Company policy or otherwise approved in writing by our General Counsel. Telephone, email, Internet and other communication means provided by the Company are to be used for business purposes. However, limited use of Company communication means for personal purposes is acceptable.

To ensure the protection and proper use of the Company's assets, each employee must: (i) exercise reasonable care to prevent theft, damage or misuse of Company property; (ii) report the actual or suspected theft, damage or misuse of Company property to a supervisor; (iii) safeguard all electronic programs, data, communications and written materials from inadvertent access by others; (iv) use Company property only for legitimate business purposes, as authorized in connection with your job responsibilities; and (v) submit accurate expense reimbursements in conformance with the Company's expense reimbursement policy.

Employees should be aware that Company property includes all data and communications transmitted or received to or by, or contained in, the Company's electronic or telephonic systems. Company property also includes all written communications. Employees and other users of this property should have no expectation of privacy with respect to these communications and data. To the extent permitted by law, the Company has the ability, and reserves the right, to monitor all electronic, Internet, and telephonic communication. These communications may also be subject to disclosure to law enforcement or government officials.

Upon termination of employment or at the company's request, employees are required to promptly return all company property, including laptops, mobile devices, access cards, documents, and any other materials or equipment issued during their employment. Failure to return company property may result in the withholding of final paychecks, legal action, or other disciplinary measures. Employees are expected to ensure that all returned items are in good condition, and any loss or damage should be reported immediately to the People & Culture department.

Information Security Roles and Responsibilities

The Information Security Officer (or designated individual) is responsible for overseeing the implementation and maintenance of Emerald's Information Security Management System (ISMS). All employees are responsible for safeguarding information assets, reporting security incidents, and complying with security controls. Managers must ensure their teams are aware of and adhere to all information security requirements relevant to their roles.

Access to information and systems is granted based on business need and is

regularly reviewed. Employees must use unique credentials and strong passwords, and must not share access credentials with others. All information assets, including hardware, software, and data, must be identified, classified, and handled according to their sensitivity and value to the company.

Fair Dealing and Competition

The Company seeks to outperform its competition fairly and honestly. Stealing proprietary information, possessing trade secret information obtained without the owner's consent or inducing such disclosures by past or present employees of other companies is prohibited. Each employee should endeavor to respect the rights of and deal fairly with the Company's customers, suppliers and competitors. No employee should take unfair advantage of anyone through manipulation, concealment, abuse of privileged information, misrepresentation of material facts or any other intentional unfair-dealing practice.

Relationships with Customers

Our business success depends upon our ability to foster lasting customer relationships. The Company is committed to dealing with customers fairly, honestly and with integrity. Specifically, you should keep the following guidelines in mind when dealing with customers:

- Information we supply to customers should be accurate and complete to the best of our knowledge. Employees should not deliberately misrepresent information to customers.
- Customer entertainment should not exceed reasonable and customary business practice. Employees should not provide entertainment or other benefits that could be viewed as an inducement to or a reward for, customer purchase decisions. Please see "Gifts and Entertainment."

Relationships with Suppliers

The Company deals fairly and honestly with its suppliers. This means that our relationships with suppliers are based on price, quality, service and reputation, among other factors. No employee should accept or solicit any personal benefit from a supplier or potential supplier that might compromise, or appear to compromise, his or her objective assessment of the supplier's products and prices. Employees can give or accept promotional items of nominal value or moderately scaled entertainment within the limits of responsible and customary business practice. Please see "Gifts and Entertainment."

Further, all third-party suppliers and service providers who have access to Emerald's information or systems must meet the company's information security requirements. Supplier security will be assessed prior to engagement and reviewed periodically. Contracts with suppliers must include appropriate information security and confidentiality clauses.

Relationships with Competitors

The Company is committed to free and open competition in the marketplace. Employees should avoid actions that would be contrary to laws governing competitive practices in the marketplace, including federal and state antitrust laws. Such actions include misappropriation and/or misuse of a competitor's confidential information or making false

statements about the competitor's business and business practices. Making critical statements about competitors that are false or misleading are disparaging and can violate the antitrust laws as well as fraud and deception laws. Encouraging a customer or prospective customer to violate the terms of a contract with a competitor could be illegal. Employees are also prohibited from discussing competitive matters with any competitors, without the prior written authorization of our General Counsel. For further discussion of appropriate and inappropriate business conduct with competitors, see "Compliance with Antitrust Laws."

Compliance with Laws, Rules and Regulations

Each employee has an obligation to comply with all laws, rules and regulations applicable to the Company's operations. These include, without limitation, laws covering bribery and kickbacks, copyrights, trademarks and trade secrets, information privacy, insider trading, illegal political contributions, antitrust prohibitions, foreign corrupt practices, offering or receiving gratuities, environmental hazards, employment discrimination or harassment, occupational health and safety, false or misleading financial information or misuse of corporate assets. You are expected to understand and comply with all laws, rules and regulations that apply to your job position. If any doubt exists about whether a course of action is lawful, you should seek advice from your supervisor or the Company's General Counsel.

Information Security Risk Management

Emerald's information security policies and controls will be reviewed at least annually and updated as necessary to ensure ongoing compliance with ISO 27001 and other applicable standards. All policies and procedures will be maintained in a controlled manner, with version history and approval records. Employees will be notified of significant changes to information security policies.

All employees and contractors will receive information security awareness training upon hire and at least annually thereafter. Training will cover Emerald's information security policies, procedures, and the importance of protecting information assets. Employees are expected to stay informed about current security threats and best practices.

Emerald will conduct regular risk assessments to identify threats and vulnerabilities to information assets. Appropriate controls will be implemented to mitigate identified risks. Employees must participate in risk assessment activities as required and promptly report any new or emerging risks to the Information Security Officer or General Counsel.

All suspected or actual information security incidents, including data breaches, must be reported immediately to the Information Security Officer or General Counsel. Incidents will be investigated promptly, and corrective actions will be taken to prevent recurrence. Employees must cooperate fully with any incident investigations.

Interactions with the Government

In the course of your duties at the Company, you may interact with the U.S., state and local governments or the governments of other countries. In any such interactions with government, you should:

- Be forthright and candid at all times. No employee should intentionally misstate or omit any material information from any written or oral communication with the government.

- Not offer or exchange any gifts, gratuities or favors with, or pay for meals, entertainment, travel or other similar expenses for, government employees. However, de minimis expenses (\$25 per person or less) for meals and entertainment are permitted so long as the intended recipient confirms that he/she is permitted to accept such a gift based on his/her employer's rules and any applicable laws. Any expenses above \$25 per person require pre-approval from the Legal Department. Regardless of value, you should avoid doing anything that would raise even the appearance of impropriety.

If your job responsibilities include interacting with the government, you are expected to understand and comply with the special laws, rules and regulations that apply to your job position. If any doubt exists about whether a course of action is lawful, you should seek advice immediately from your supervisor or the Company's General Counsel. See "The Foreign Corrupt Practices Act" for a more detailed discussion of the Company's policies regarding interactions with governments of other countries.

The Foreign Corrupt Practices Act

The Foreign Corrupt Practices Act (the "FCPA") prohibits the Company and its employees, directors and agents from offering or giving money or any other item of value to win or retain business or to influence any act or decision of any government official, political party, candidate for political office or official of a public international organization (i.e. the payment of bribes, kickbacks or other inducements to a foreign official is prohibited). The law assumes that any of these persons may be in a position to influence buying decisions in favor of the person paying the bribe. This prohibition also extends to payments to a sales representative or agent if there is reason to believe that the payment will be used indirectly for a prohibited payment to foreign officials. Violation of the FCPA is a crime that can result in severe fines and criminal penalties, as well as strict disciplinary action by the Company, including termination of employment or engagement.

Certain small facilitation payments to foreign officials may be permissible under the FCPA if legal and customary in the country or locality and intended to secure expedited routine governmental action. Governmental action is "routine" if it is ordinarily and commonly performed by a foreign official and does not involve the exercise of discretion. For instance, "routine" functions would include setting up a telephone line or expediting a shipment through customs. To ensure legal compliance, any facilitation payments, whether or not covered by the FCPA, must receive prior written approval from the Company's Chief Financial Officer and General Counsel and must be clearly and accurately reported as a business expense.

The FCPA also regulates the Company's accounting practices in all countries to make it easier to prevent bribes and uncover illegal transactions. No undisclosed or unrecorded funds or assets may be established or maintained for any purpose, no false or artificial entries may be made in any books or records of the Company for any reason, and no payment may be approved or made with the intention or understanding that it is to be used for any purpose other than that described by the document supporting the payment.

Employees who are asked by a customer, supplier, government official or other party to make or to take a bribe, kickback or other prohibited payment or gift, should refuse the request, and immediately inform their supervisor and the General Counsel.

For a more detailed discussion regarding the FCPA, see the Company's FCPA and Anti-Bribery Policy.

Employment Practices

Harassment and Discrimination

The Company values its employees' individual and collective capabilities. It employs, trains, promotes and compensates individuals based on job-related qualifications and abilities, without regard to, for example, race, color, religion, national origin, gender, sexual orientation, age, marital status or other characteristic protected by law.

The Company has a strong commitment to maintaining a bias-free environment where harassment is prohibited. Harassment can include any action that interferes with an employee's work performance or creates an environment that is offensive, intimidating or hostile to work in. The Company will not tolerate harassment of any kind of our employees, including sexual harassment.

Sexual harassment occurs when decisions affecting an individual, such as hiring, firing, promotions, awards, and transfers or disciplinary action are influenced by the submission to or rejection of unwelcome sexual advances. Sexual harassment can also include actions that create a hostile or offensive environment for members of a given sex, whether the act is perpetrated by a supervisor or by a co-worker. Courteous, mutually respectful, pleasant, non-coercive interactions between employees that are acceptable to both parties should be the norm in all our dealings with one another. Each supervisor and employee has an affirmative duty to try to keep his or her workplace free of harassment, including sexual harassment and intimidation. Supervisors must make clear that no one is required to endure insulting, degrading or exploitive treatment. If any employee believes that they are being harassed, they should talk to their supervisor, a Human Resources representative or the General Counsel, or make an anonymous call to the Whistleblower Hotline.

Alcohol and Drugs

Emerald is committed to maintaining a healthy and productive work environment. The use, possession, or distribution of alcohol, tobacco, or illegal drugs is strictly prohibited on company premises and during work hours, except where alcohol consumption is specifically authorized at approved company events. Employees are expected to comply with all applicable laws regarding substance use while representing Emerald.

Any employee found to be under the influence of alcohol or drugs while at work or engaging in the unauthorized use or distribution of such substances, will be subject to disciplinary action, up to and including termination of employment. Exceptions for alcohol use may be made for company-sponsored events, but employees are expected to exercise moderation and professional conduct at all times. The use, possession, or being under the influence of illegal drugs while working, at Company and client events, and/or if off-duty activity affects an employee's work performance or the Company's business, is strictly prohibited. "Illegal drugs" are defined as controlled substances that are not legally obtainable or not obtained in a lawful manner. Also, Employees should not report to work under the influence of any legal drug that might affect their safety or the safety of others. "Legal drugs" are legally obtained prescribed or over-the-counter drugs that are used for the purpose for which they were prescribed and sold.

The use of marijuana and/or psychedelics is prohibited during work hours, on Company premises, and at any Company-sponsored events unless it is for verified medical reasons.

Employees who have a medical need to use marijuana or medically related psychedelics must provide appropriate documentation to People & Culture to ensure reasonable accommodation can be made

Emerald encourages employees who may be experiencing issues related to alcohol or substance dependency to seek assistance. The company offers support and resources for those who voluntarily come forward, and such requests for help will be treated with confidentiality and respect. The overarching goal of this policy is to ensure the safety, well-being, and professionalism of the entire workforce.

Use of Mobile Devices While Driving

The safety of Company employees, and those who may be impacted by the actions of Company employees while on duty or in conjunction with work, is vitally important. Therefore, the Company strictly prohibits the use of mobile devices while driving a Company vehicle or any vehicle on Company business, including commuting to and from work; provided, however, that if the laws of the state in which you are driving allow for hands free use of a mobile device, the Company does not prohibit such lawful use, however, the Company does discourage such use. Subject to the foregoing exception and any applicable laws to the contrary, the Company also strictly prohibits using a mobile device, while driving anywhere and at any time, in order to read or send Company email or text messages, to make or receive business-related phone calls, or to search the Internet for business-related purposes. It is the Company's policy that, in the interest of safety, business-related emails, texts, phone calls, and Internet use should be dealt with either before or after driving.

Violence and Weapons

The Company will not tolerate violence or threats of violence in, or related to, the workplace. If you experience, witness or otherwise become aware of a violent or potentially violent situation that occurs on the Company's property or affects the Company's business you must immediately report the situation to your supervisor or the Human Resources Department.

The Company does not permit any individual to have weapons of any kind on Company property or in vehicles, while on the job or off-site while on Company business. This is true even if you have obtained legal permits to carry weapons. The only exception to this policy applies to security personnel who are specifically authorized by Company management to carry weapons.

Social Media Uses

Emerald's Social Media Policy applies to all employees and contingent workers, providing guidance and rules for both professional and personal use of social media platforms. Employees must avoid making statements that could be construed as representing the company or disclosing material non-public information. Personal use of social media should not occur during work hours or on company devices, and employees are encouraged to use privacy controls and keep work relationships separate from personal networks.

When engaging in social media activities, employees should support legal compliance by refraining from sharing confidential or sensitive company information, commenting on ongoing litigation, or jeopardizing contractual obligations. Any content created, contributed, or distributed via social media—whether through company or personal accounts—must adhere to

these guidelines, and employees should be mindful that new platforms and technologies are also covered by the policy.

If employees have questions about the policy or encounter issues, they should contact the People and Culture team for guidance. The company reserves the right to revise the policy as needed, and employees are expected to stay informed about updates. Violations of the policy may result in disciplinary action

Remote Work

Emerald's Remote Work Policy provides employees with the flexibility to work from home, on the road, or at a satellite location for all or part of their workweek, when both the employee and the job are suited to such an arrangement. Remote work is considered a viable option for certain roles and individuals but is not guaranteed for any position. The policy clarifies that remote work does not change the terms and conditions of employment with Emerald. Arrangements can be either informal, such as for short-term projects or business travel, or formal, involving a set remote schedule. Either the employee or the manager may propose a remote work arrangement, and any such arrangement may be discontinued at will by either party. While Emerald will make every effort to provide 30 days' notice before ending a remote work arrangement, there may be circumstances where no notice is possible.

Eligibility for remote work generally requires that the employee has been with Emerald for at least six months and has a satisfactory performance record, unless the position is designated as remote at the time of hire. Before entering into a permanent remote work agreement, the employee and manager must evaluate the suitability of the arrangement, considering job responsibilities, equipment and workspace needs, scheduling, and the employee's skills and performance. The arrangement must also be reviewed with the People & Culture Business Partner to ensure compliance with all company policies and legal requirements.

Employees working remotely who are not exempt from overtime requirements of the Fair Labor Standards Act are required to accurately record all hours worked using the company's time-keeping system. Non-exempt employees must obtain advance approval from their manager for any overtime. Failure to comply with timekeeping requirements may result in immediate termination of the remote work agreement. Equipment needs will be determined on a case-by-case basis, with Emerald supplying and maintaining necessary business equipment. All company property must be returned upon termination of employment. Employees are responsible for setting up an appropriate and safe work environment at their remote location, but Emerald does not cover costs associated with home office setup, such as furniture or remodeling. Office supplies may be obtained from the office or delivered for bulk needs, but employees will not be reimbursed for supplies purchased independently.

Remote employees are expected to maintain the security of proprietary company and customer information, including using locked storage, regular password maintenance, and secure access to company systems, such as VPNs. Any customer personally identifiable information (PII) should be stored only on Emerald systems. Employees must also maintain a safe workspace, as injuries sustained while working remotely in connection with regular duties are generally covered by the company's workers' compensation policy. Employees are responsible for promptly reporting any such injuries. The policy also clarifies that remote work is not intended as a replacement for appropriate childcare; while schedules may be adjusted to accommodate childcare needs, job performance and business demands must remain the primary focus. For any questions or concerns about remote work, employees are encouraged to contact

their People & Culture Business Partner.

Address Change

All Emerald employees are required to inform the P&C team via email of any changes to their home address. This includes both permanent and temporary address changes. A temporary address change includes anywhere you plan on living for more than 30 days but for less than 6 months.

If you are planning on a state-to-state change of permanent residence or moving to another country, you will need *approval from the P&C team* and your direct manager before the move.

Employee Privacy

Access to personal information about Company employees, for which they would have a reasonable expectation of privacy, is restricted to employees with a “need to know” within the Company and will be transmitted to other employees or third parties only for legitimate and necessary business purposes or to satisfy legitimate investigative or legal requirements. Employees who are responsible for maintaining personal information must ensure that the information is not disclosed inappropriately or misused.

Environmental, Health and Safety

The Company is committed to providing a safe and healthy working environment for its employees and to avoiding adverse impact and injury to the environment and the communities in which it does business. Employees must comply with all applicable environmental, health and safety laws and regulations. It is each employee’s responsibility to understand and comply with the laws, regulations and policies that are relevant to his or her job. Failure to comply with environmental, health and safety laws and regulations can result in civil and criminal liability against the offending employee and the Company, as well as disciplinary action by the Company, up to and including termination of employment. You should contact the Company’s General Counsel with questions about the applicable laws, regulations and policies.

Environment

All employees should strive to conserve resources and reduce waste and emissions through recycling and other energy conservation measures. All employees are required to comply with all applicable environmental laws and regulations relevant to their positions. Everyone is expected to promptly report any known or suspected violations of environmental laws or any events that may result in a discharge or emission of hazardous materials.

Health and Safety

The Company is committed not only to complying with all relevant health and safety laws, but also to conducting business in a manner that protects the safety of its employees. All employees are required to comply with applicable health and safety laws and regulations. Concerns about unsafe conditions or tasks that present a risk of injury are to be reported immediately to a supervisor or the Company’s General Counsel.

Compliance with Antitrust Laws

Antitrust laws of the United States and other countries are designed to protect consumers and competitors against unfair business practices and to promote and preserve competition. The general aim of these laws is to promote competition and let businesses compete on the basis of quality, price and service. Our policy is to compete vigorously and ethically while complying with all antitrust, monopoly, competition or cartel laws in all countries, states or localities in which the Company conducts business. Violations of antitrust laws may result in severe penalties against the Company and its employees, including potentially substantial fines and criminal sanctions. You are expected to maintain basic familiarity with the antitrust principles applicable to your activities, and you should consult the Company's Chief Financial Officer or General Counsel with any questions you may have concerning compliance with these laws.

The following is a summary of actions that are violations of applicable antitrust laws:

Price Fixing. The Company may not agree with its competitors to raise, lower or stabilize prices or any element of price, including pricing policies, bids, costs, discounts, promotions, terms and conditions of sale, credit terms, freight charges or royalties. The basic rule in determining prices is simple: the Company must, on its own, determine the price and conditions of sale of its products and services based on its costs, market conditions and experience in the marketplace.

Limitation of Supply. The Company may not agree with its competitors to limit its quantity or type of production or restrict the supply of its services.

Allocation of Territories or Customers. The Company may not agree with its competitors to sell or refrain from selling in any geographic area or to any customers or class of customers, or to divide or share a customer's business.

Boycotts and Refusal to Deal. The Company may not agree with its competitors, suppliers or customers to refuse to sell or purchase products from third parties. In addition, the Company may not prevent a customer from purchasing or using non-Company products or services. Generally, the Company has the right to refuse to buy from or sell to anyone; however, it must reach such decisions independently without consulting with a competitor.

Tying. The Company may not require a customer to purchase a product that it does not want as a condition to the sale of a different product that the customer does wish to purchase, especially if the latter product has a dominant market share.

Meetings with Competitors

Employees should exercise caution in meetings with competitors. Any meeting with a competitor may give rise to the appearance of impropriety. As a result, if you are required to meet with a competitor for any reason, you should obtain the prior approval of the Chief Financial Officer or General Counsel. You should try to meet with competitors in a closely monitored, controlled environment for a limited period of time. You should create and circulate agendas in advance of any such meetings, and the contents of your meeting should be fully documented. Specifically, you should avoid any communications with a competitor regarding: Prices; Costs; Market share; Allocation of sales territories; Profits and profit margins; Supplier's terms and conditions; Product or service offerings; Terms and conditions of sale; Bids for a particular contract or program; Selection, retention or quality of customers; Distribution methods or channels; Marketing strategies; Future development plans or product roadmaps; or Other

subjects relating to or affecting the production or sale of products to existing or prospective customers.

If you participate in a meeting with a competitor in which any of the above topics are broached, you should affirmatively end the discussion, and you should state your reasons for doing so. During meetings with competitors, avoid sharing or obtaining confidential information from the competitor. Also avoid statements that could be construed as unfair acts such as harassment, threats or interference with the competitors' existing contractual relationships.

Professional Organizations and Trade Associations

Employees should be cautious when attending meetings of professional organizations and trade associations at which competitors are present. Attending meetings of professional organizations and trade associations is both legal and proper, if such meetings have a legitimate business purpose and are conducted in an open fashion, adhering to a proper agenda. At such meetings, you should not discuss the restricted topics listed above, the Company's pricing policies or other competitive terms or any other proprietary, competitively sensitive information.

Discussions and Communications

The illegal practices outlined above need not take the form of official or written agreements. Any kind of casual understanding between two companies that a business practice adopted by one and followed by the other may be used in court as evidence of an illegal agreement. You should avoid contact of any kind with competitors that could create the appearance of improper agreements or understandings. Even social conversations can be used as evidence that an agreement existed. Memos and other written communications that use casual or inappropriate language might be examined by a government agency or opposing lawyers. Employees who find themselves in a situation where customers or pricing is raised in discussions with competitors should clearly state that they will not participate in price or similar discussions.

Political and Charitable Activities

The Company recognizes the legitimate interests of employees in being involved in political activities, including the support of political candidates and the expression of opinions on political or public issues. Similarly, the Company recognizes and encourages employees' involvement in charity and community service and the making of charitable donations. However, employees should make it clear that they are acting or speaking on their own behalf and not on behalf of the Company in engaging in such activities or making such donations. Federal and state contribution and lobbying laws severely limit the contributions the Company can make to political parties or candidates. Donations of Company funds or assets and the use of the Company's name in support of political or charitable causes may only be made with prior written approval by the Company's Chief Executive Officer or Chief Financial Officer. Otherwise, any political activity you pursue must be done voluntarily and using your own resources and time outside of working hours.

Insider Trading Laws

Employees who obtain material, non-public information about another company, including the Onex Corporation, in the course of their duties are prohibited from trading in the stock or securities of the other company while in possession of such information or “tipping” others to trade on the basis of such information. Violation of insider trading laws can result in severe fines and criminal penalties, as well as disciplinary action by the Company, up to and including termination of employment.

The same restrictions apply to others living in the household of employees and family members of employees; employees are expected to be responsible for their compliance as well. ‘Material’ information is generally regarded as information that a reasonable investor would think important in deciding whether to buy, hold or sell the security; in short, it is any information that could reasonably affect the price of the security. Examples of potentially material information include sales results, earnings, dividend actions, strategic plans, new products, important personnel changes, acquisition and divestiture plans, the gain or loss of a major client, marketing plans and joint ventures, and government actions. “Nonpublic” means information that has not been made public. Additional information regarding avoiding insider trading is available in the Company’s Securities Trading Policy.

Public Communications and Fair Disclosure

Public Communications Generally

The Company places a high value on its credibility and reputation in the community. What is written or said about the Company in the news media and investment community directly impacts our reputation, positively or negatively. Any information we provide must be accurate and complete, consistent with our obligations to maintain the confidentiality of competitive and proprietary information and to prevent selective disclosure of market-sensitive financial data. To that end, all news media or investment community requests for information regarding the Company should be directed to the Chief Financial Officer.

Fair Disclosure

The Company has outstanding debt securities which are bought and sold from time to time, and it is illegal for an investor to buy or sell Company debt securities on the basis of “material nonpublic information.”

Accordingly, the Company should not be disclosing material information about the Company to market segment analysts or reporters, securities market professionals or debt holders that has not been made available to all investors in the Company’s debt securities through the bondholder website and any other means.

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

A non-exhaustive list of information that could be material includes: Company earnings forecasts, quarterly or annual results in advance of publishing them on the bondholder website or any other means, the results of large tradeshows, starting new or shuttering existing tradeshows, and significant transactions contemplated by the Company (for example, acquisitions and dispositions).

Waivers

The Company may waive certain provisions of the Code of Business Conduct and Ethics when deemed appropriate under the circumstances. Any employee who believes that a waiver may be called for should initially discuss the matter with any one of the Company's Chief Executive Officer, Chief Financial Officer, or General Counsel. Waivers for directors and officers of the Company may be made only by the Board of Directors or the Audit Committee of the Board and, if required by law or New York Stock Exchange rules and regulations, will be promptly disclosed to the public.

Consultation, Reporting and Retaliation

Employees should report all violations of law, regulation or this Code of which they become aware to any one of the Company's Chief Executive Officer, Chief Financial Officer, or General Counsel, or if desired, to the Chair of the Audit Committee. Similarly, any employee who is unsure as to whether a violation has occurred or who needs guidance as to whether to take a particular action that may be, or may appear to be, a violation, should consult any of those individuals. This policy outlines the standards and procedures by which Company employees should report instances of non-compliance. Employees at every level, in every department, and at every location have a responsibility to speak up when they believe they have knowledge of the Company or one of its employees being out of compliance.

The Company prohibits retaliation against an employee who, in good faith, seeks help or reports known or suspected violations. Any reprisal or retaliation against an employee because the employee, in good faith, sought help or filed a report will be subject to disciplinary action, including potential termination of employment. Employees should review the Company's Whistleblower Policy for details as to suspected or known violations and how to report a concern, including the procedure for confidential, anonymous reporting, and the protections to which they are entitled in making such a report. Knowingly failing to report a violation is a violation of the Code in itself.

Consequences of Violation

A failure to abide by the Code, including a violation, helping or encouraging another to violate the code, knowingly failing to report a violation or retaliating against someone who reported a violation, may result in disciplinary action by the Company that takes into account the seriousness of the violation and the conduct of the employee in response thereto. Self-reporting by employees is encouraged and will be given due consideration by the Company in dealing with any violation. Disciplinary action may include verbal warnings, written reprimands, suspension or dismissal from employment, and in some cases, referral for criminal prosecution. Additionally, the Company may pursue any and all remedies available to it for damages suffered by the Company resulting from a violation of the Code. The appropriate disciplinary action will be determined by management in its discretion based on the circumstances and nature of the violation in each case. While it is the intention of the Company that the Code be applied even-handedly and that all

employees be treated fairly and equally, there should be no expectation that discipline applied in one case will be the same as was applied in any other case, and no employee shall have any claim for relief from disciplinary action based on the treatment received by another employee in a similar case.

Conclusion

This Code and the matters contained herein are neither a contract of employment nor a guarantee of continuing Company policy. The Company reserves the right to amend, supplement or discontinue this Code and the matters addressed herein, without prior notice, at any time.

I certify that I have read, understand, and agree to the terms of this policy/agreement, and I hereby acknowledge it:

SIGNATURE:

DATE: