NTT DATA Services
Global Code of Business Conduct

Version 1.0 - September 2022

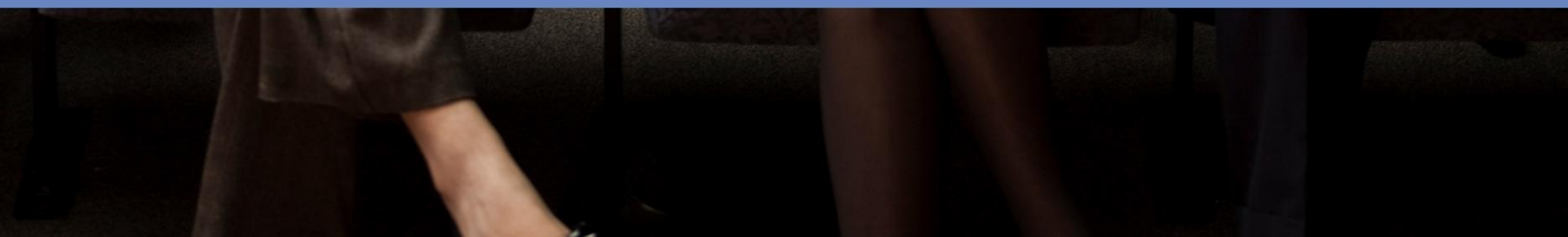

TABLE OF CONTENTS

1 Introduction to the Global Code of Business Conduct

1.1 Welcome Statement - A Message to all Employees

To NTT DATA Services employees,

The Global Code of Business Conduct – the "Code" -- reminds each of us to diligently protect NTT DATA Services ("Company") by conducting business in accordance with the highest ethical practices. We also must ensure that in every work setting, our actions comply with all applicable laws, regulations and Company policies.

The Code explains our standards and discusses common and recurring issues along with appropriate responses. Please read it carefully. Of course, no single document can address every possible situation, and potential conflicts of interest and other concerns constantly evolve. I encourage you to seek assistance whenever necessary. You can discuss concerns and report possible violations through numerous available channels, as outlined in the Code.

I am exceedingly proud of our Company, our colleagues, our culture & values and our reputation and leadership position in the market. In all things, we set a high standard for working with excellence and integrity. As a result, we're delivering substantial value to our clients, driving greater diversity and inclusion, creating fulfilling career and development opportunities for teamates, supporting our communities, and delivering solid returns to our shareholders. Sustaining and building upon this foundation, we all must continue doing the right things in the right way which is clearly outlined in our annual Code training.

I encourage you to complete the course at your earliest opportunity, well in advance of our expected completion date.

Sincerely,

Bob Pryor
Chief Executive Officer NTT DATA Services[1]

[1] NTT DATA Services includes NTT Data International L.L.C. and NTT DATA Services International Holdings B.V. and their respective subsidiaries, as well as NTT DATA (China) Co. Limited, Dalian Branch and, to the extent related to NTT DATA Services, PT NTT DATA Indonesia and NTT DATA (Thailand) Co., Ltd. In this Code, the foregoing entities and business units shall collectively be referred to as NTT DATA.

1.2 NTT DATA Group Code of Conduct

NTT DATA Corporation (Global Headquarters of NTT DATA Group) has its own code of conduct which describes basic standards and values for NTT DATA Group companies and their employees. Our Company has adopted the NTT DATA Group Code in addition to the Code. Included within the NTT DATA Group Code are core principles, including:

- **Ethical and Responsible Business Activities**
  - NTT DATA Group complies with applicable laws and regulations in the countries and regions where it does business, and have zero tolerance for any form of corporate criminal offences and illegal misconducts. Furthermore, NTT DATA Group respects international standards and acts in a highly ethical manner, in accordance with the social responsibility expected of a global company. These are our fundamental principles of behaviors necessary for NTT DATA Group to gain trust from society, enhance our corporate values, and safeguard our own sustainable development. We engage in our day-to-day business activities always in accordance with our fundamental principles.
- **Respect for Human Rights**
  - NTT DATA Group complies with the Universal Declaration of Human Rights and other international treaties and conventions which are discussed and adopted from a global perspective, as common standards that all people and countries should achieve. As a member of NTT Group, NTT DATA Group understands fully and strives to realize the NTT Group Global Human Rights Policy, which is part of NTT Group's core policies.
  - NTT DATA Group endeavors not to cause or exacerbate any negative impact on human rights in the course of our business activities, and will not tolerate any forced labor or child labor. Further, NTT DATA Group endeavors to introduce and implement human rights due diligence procedures to identify and take measures on the risks concerning human rights, and to take serious action to resolve negative consequences to human rights. * For details: NTT Group Global Human Rights Policy: https://group.ntt/en/newsrelease/2021/11/10/pdf/211110ca.pdf
- **Diversity, Equity & Inclusion**
  - NTT DATA Group believes DEI (Diversity, Equity and Inclusion) is essential, because promoting and realizing DEI will bring about innovation in the world and lead to the sustainable growth and development of society. DEI is an environment in which people with diverse personalities, backgrounds, perspectives and values respect each other (Diversity), work under fair opportunities and conditions according to their circumstances (Equity), and each person makes the most of themselves to work in cooperation with each other (Inclusion).
  - We respect all people (such as clients, business partners and Employees) with diverse personalities, backgrounds, perspectives, and values. NTT DATA Group will endeavor to foster a society where Employees can utilize their respective talents, share their wisdom, and thrive through cooperating with all people.
- **Global Environmental Issues**
  - NTT DATA Group endeavors to do its part with respect to global environmental issues for the benefit of all people and future generations through the Group's businesses and corporate initiatives. We aim not only to become carbon neutral throughout the NTT DATA Group value chain, but also to achieve carbon neutral status for our clients and society at large by means of green innovation that utilizes IT. We will create a sustainable environment by working together with various stakeholders for achieving goals including circular economy and nature conservation.

- **Responsible Value Chain**
  - NTT DATA Group acts and strives, together with our clients and business partners, to address various social issues related to human rights, labor, environment and corrupt practices that may occur not only within the Group but also on our value chain. We endeavor to contribute to realizing a sustainable society by sufficiently communicating with our clients and business partners and building a responsible value chain by evaluating the impact on society of the products and services we procure and the solutions we provide.

Please review the entire NTT DATA Group, which can be found on the NTT DATA Group website. Our Code is designed to be congruent and complementary with the NTT DATA Group Code, but if you have any questions about the applicability of either code, please contact the Compliance Team.

1.3 Policy Statement Concerning the Global Code of Business Conduct

It is the Company's policy to conduct its affairs in accordance with the highest moral and ethical principles and to comply with all applicable laws and regulations. This Code sets forth legal and ethical standards of conduct for officers and employees (collectively referred to as "Employees") of the Company. Although it is the purpose of the Code to present a clear statement of what is expected of all Employees, the Code cannot address all possible situations of concern that may arise. Accordingly, the Company has put a number of other policies and procedures in place to try to fill these gaps.

Employees are expected to be aware of this Code and the Company's policies and procedures and to act in accordance with them at all times. Employees are expected to use good judgment and common sense in seeking to comply with this direction, and to ask for advice when they are uncertain. This Code applies to the Company and all of its subsidiaries and other business entities controlled by it worldwide.

1.4 Responsibilities

- The Company has the duty to communicate to all Employees the standards of ethics and conduct set forth in this Code and to enforce these standards at all levels.

- Every Employee of the Company has the duty to read, understand, and comply with this Code. Any Employee who has questions about, or suspects violations of, the Code must follow the Reporting Concerns as outlined in Section 2.1 below.

- The Company requires that all Employees, directors, contractors and agents comply with all laws, rules and regulations applicable to the Company wherever it does business. If anyone becomes aware of the violation of any law, rule or regulation by the Company, whether by its directors, officers, Employees, or any third party doing business with or on behalf of the Company, it is the Employees' responsibility to promptly report the matter to their leader or to the Compliance and Disclosure Committee (the "Compliance Team") or if necessary to a Division Leader. While it is the Company's desire to address matters internally, nothing in this Code should discourage anyone from reporting any illegal activity, including any violation of the securities laws, anti-bribery and corruption laws, antitrust laws, and environmental laws or any other federal, state or foreign law, rule or regulation, to the appropriate regulatory authority. Employees and directors shall not discharge, demote, suspend, threaten, harass or in any other manner discriminate or retaliate against an Employee because the Employee in good faith reports any such violation. This Code should not be construed to prohibit Employees from testifying, participating or otherwise assisting in any state or federal administrative, judicial or legislative proceeding or investigation.

- Leaders of the Company have the duty to make certain that all Employees under their supervision are advised of the current provisions of this Code and are periodically reminded of the importance of adhering to the principles set forth in it, and to create and maintain an environment where each Employee feels responsible for and comfortable with complying with this Code and reporting actual or suspected violations of it, without fear of retribution or retaliation.

2 Our Work Environment

2.1 Reporting Concerns

Anyone having knowledge of, or questions or concerns about, an actual or possible violation of the provisions of this Code must immediately report the matter to their immediate leader or via one of the options below.

- Online via the "Report Online" portal: https://nttdata.i-sight.com/landing-page
- By phone: Continental US and Canada dial 1-855-399-6120 and in Mexico dial 1-800-522-6497.
- For a list of phone numbers for other locations reference the "Report Online" portal at https://nttdata.i-sight.com/landing-page
- The Compliance Team, via the "Report Online" portal: https://nttdata.i-sight.com/landing-page
- The Employee Relations CoE
- The HR Business Partner assigned to your team
- Internal Audit

Remember, if an Employee does not feel comfortable talking to their leader about a known or suspected violation of NTT DATA policy or the law, for instance because their leader already knows of or has approved the conduct in question, the Employee nevertheless needs to report such matter through one of the above alternative avenues. Similarly, if an Employee is not comfortable with the response they received or the action taken by their leader, they need to elevate such issue by one of the above alternative avenues.

NTT DATA strictly prohibits discrimination or retaliation in any form against Employees for making good faith reports of their concerns.

2.2 Equal Opportunity

The Company is dedicated to the fair and equal treatment of its Employees and to providing employment opportunities on the basis of individual merit, consistent with local laws. To that end, the Company condemns and will not tolerate discrimination against its Employees or applicants on the basis of race, color, national origin, religion, sex, sexual orientation, disability, age, genetic information, ancestry, marital status, veteran status, creed, citizenship status, gender identity or expression or other basis protected by applicable law, including, without limitation, United States federal, state and local laws. The Company's nondiscrimination policy applies to recruitment, hiring, training, compensation, benefits, promotion, demotion, transfer, termination and all other terms, conditions and privileges of employment.

Additionally, and consistent with applicable law, the Company will make reasonable accommodation for qualified individuals with disabilities unless doing so would result in an undue hardship to the Company. An applicant or Employee who requires an accommodation in order to perform the essential functions of the job should contact their management team, or a human resources representative, to request such an accommodation.

Any Employee who has any questions, issues, or suggestions concerning this policy should contact their leader, the Compliance Team, or the HR Business Partner assigned to the Employee's business unit.

2.3 Security Obligations

All Employees have a right to work in an environment that is safe, secure, and free of violence. Employees have an obligation to work with the Company to achieve this goal by supporting access control practices, wearing Company identification, escorting visitors, and reporting unauthorized or suspicious activity and persons to their management or to the facilities manager if at a corporate office. Certain of the Company's customers and subsidiaries have more detailed security policies and procedures, which Employees are obligated to understand and follow when performing work for such customers and subsidiaries.

2.4 Policy Against Harassment

The Company is committed to providing a productive and professional work environment. Accordingly, harassment of Employees occurring in the workplace or other work-related settings that is based on race, color, national origin, religion, sex, sexual orientation, disability, age, genetic information, ancestry, marital status, veteran status, creed, citizenship status, gender identity or expression or other basis protected by federal, state, local, or other applicable laws, will not be tolerated by the Company. Similarly, sexual harassment occurring in the workplace or other work-related settings will not be tolerated by the Company. Each Employee is responsible for treating other Employees with dignity and respect and ensuring that their personal conduct and comments in the workplace support a professional environment that is free from unlawful harassment.

Any incident of harassment should be reported to the Employee's leader, the HR Business Partner assigned to the Employee's business unit, the Compliance Team, or by calling the Company's Ethics Hotline. Leaders who receive complaints or who observe harassing conduct should immediately inform Human Resources.

Complaints of harassment or other unlawful behavior are serious matters. The Company expects Employees to report such behavior and leaders to promptly act upon such allegations. If an investigation confirms improper conduct, the Company will take appropriate action. It is a violation of this policy to retaliate against any Employee for filing a good faith complaint of harassment or for cooperating in good faith in an investigation of such a complaint.

Employees should also familiarize themselves with any local Company Policy Against Harassment specific to their country or location.

2.5 Drugs and Alcohol

It is the intent of the Company to maintain a workplace that is free of illegal drugs and alcohol and to discourage drug and alcohol abuse by its Employees. The Company specifically prohibits the following acts while in the workplace or on Company business:

- The unauthorized use, possession, purchase, sale, manufacture, distribution, transportation, or dispensing of alcohol, illegal drugs, or other controlled substances;
- The purchase, sale, manufacture, distribution, transportation, or dispensing of any legal prescription drug in a manner inconsistent with law;
- Being under the influence of illegal drugs;
- Being under the influence of alcohol while working. In certain limited instances, such as at NTT DATA sponsored events or during a business-related dinner, moderate use of alcohol may be permitted, but in all such instances proper business decorum must be maintained; or
- Working while impaired by the use of a legal drug whenever such impairment might endanger the safety of the Employee or some other person, pose a risk of significant damage to Company property, or substantially interfere with the Employee's job performance.

In certain instances, such as when working in a safety-sensitive position, Employees and/or applicants may be requested to take a drug test, to the extent permitted by applicable law. In addition, Employees and applicants may be required to submit to drug and alcohol testing, to the extent permitted by applicable law, before being permitted to work on certain customers' projects, at the customers' request.

All Employees should familiarize themselves with the Company's Drug-Free Workplace Policy. Among other requirements, if an Employee is convicted of violating a drug statute while on Company property or business, and that Employee is assigned to work under a government contract, that Employee must report this fact to their leader within five days of the conviction.

2.6 Global Health & Safety

It is the Company's policy to conduct its business in a manner compliant with applicable health and safety laws and regulations. The Company is committed to continuous efforts to identify and eliminate or manage safety risks associated with our activities. For additional information pertaining to health and safety matters, please see the NTT DATA Group Code of Conduct, Section 2.3 and NTT DATA Services Global Workplace Health and Safety Policy which further addresses this important issue.

3 Conflicts of Interest

3.1 Activities Outside the Company

Generally, the Company has no interest in preventing Employees from engaging in lawful activities during non-working hours. However, Employees must make sure their outside activities do not conflict or interfere with their responsibilities to the Company. A conflict of interest occurs or may occur when a personal interest interferes, or potentially interferes, with the interests of the Company. For purposes of considering conflicts of interest, the term “Family Member” includes immediate family members, including individuals related by marriage, or members of the Employee’s household.

If an Employee has a question about a potential conflict of interest, the Employee should discuss it with their leader or the Compliance Team. Directors and certain other employees of the Company must follow the approval requirements spelled out later in this Section, at section 3.7.

For example, Employees generally may not:

- Engage in self-employment or perform paid or unpaid work for others in a field of interest similar to or competitive with services provided, or products sold, by the Company.
- Use proprietary or confidential Company information for personal gain or to the Company’s detriment or take or try to take personal advantage of a business opportunity discovered through their employment with the Company.
- Use proprietary or confidential information of competitors.
- Use Company assets or labor for personal use.
- Acquire any interest in property or assets of any kind for the purpose of selling or leasing it to the Company.
- Appear to represent the Company as the participant in an outside activity unless the Company has explicitly authorized the Employee to represent the Company.

Employees should exercise caution before deciding to serve on the Board of Directors of a for-profit company, or any Advisory Boardof any for-profit enterprise. If an Employee has any questions as to whether such a position constitutes an actual or perceived conflict of interest they should discuss it with their leader or a member of the Compliance Team. Officers and directors of the Company must follow the approval requirements outlined in Section 3.7 below.

3.2 Community Activities

The Company encourages all Employees to be actively involved in their communities through volunteer service to charitable, civic, and public service organizations and through participation in the political process.

Employees must make sure, however, that their service is consistent with their employment with the Company and does not pose an actual or perceived conflict of interest. This is particularly important before accepting any leadership position (such as membership on the board of a charitable or civic organization) and before seeking or accepting political office.

3.3 Relationships with Employees

Due to the potential for conflicts of interests, Family Members or any person with whom an Employee has a close personal relationship, such as domestic partner or dating partner, are not permitted to work in positions that have a direct reporting relationship to each other or that occupy a position in the same line of authority where one Employee makes decisions involving a direct benefit to the other Employee (each, a "Personal Relationship"). Such decisions can include, but are not limited to, hiring, retention, transfer, promotion, compensation and leave of absence requests. An Employee in such a Personal Relationship should inform an appropriate member of the Compliance Team or leader and/or a Human Resources Business Partner (i.e., someone outside of the Personal Relationship) to mitigate any actual or perceived conflicts of interests.

In some circumstances, the Company reserves the right to apply this policy to situations where there is a conflict or the potential for conflict because of the relationship between an Employee and another Employee, director, shareholder, or customer, even if there is no direct reporting relationship, but where, in the sole discretion of the Company, there is the potential for an actual or perceived conflict of interest.

3.4 Relationships with Suppliers and Customers

In dealing with suppliers, potential suppliers, customers and members of the financial community (such as underwriters and analysts), Employees may not engage in any activity which creates or appears to create a conflict between their personal interests and the interests of the Company.

It is not feasible to describe all situations in which a conflict of interest could arise in the course of dealing with suppliers, potential suppliers, customers, or members of the financial community. Some of the more common conflicts that Employees should avoid include the following:

- Accepting inappropriate personal gifts or entertainment from suppliers, potential suppliers, customers, or members of the financial community. This Code contains a separate section entitled "Gifts, Gratuities, Entertainment, and Other Considerations" that addresses this subject in detail.

- Participating in, effecting, or influencing a transaction where the supplier, potential supplier, customer, or member of the financial community is a relative or Family Member of the Employee.

- Serving as an Employee, consultant, advisor, or director of, or maintaining a material financial investment in any supplier, potential supplier, customer, or member of the financial community.

3.5 Relationships with Competitors

Employees must avoid conflicts of interest or even the appearance of a conflict of interest in their relationships with competitors. Employees may not:

- Maintain, or permit any Family Member to maintain, a material financial investment in the business of a Company competitor.
- Provide compensated or uncompensated services to a competitor, except for services rendered under a valid Company contract.
- Disclose any Company Confidential Information (defined in Section 4.12 below) to a competitor unless the competitor is also an actual or potential supplier or customer of the Company and the disclosure has been approved by appropriate Company management and a nondisclosure agreement is in place.
- Utilize for any unauthorized purposes or disclose to a competitor or other third-party any Confidential Information that has been entrusted to the Company by a customer or supplier.
- Use proprietary or confidential information of a competitor. For example, if an Employee were to receive confidential competitor information (such as a pricing proposal), by mistake or intentionally, from a client or someone else, they should not review such information, distribute it or otherwise use it. Instead, they should immediately contact their leader, the Corporate Legal Department, and/or the Compliance Team for guidance on how to proceed.

Relationships with competitors may, under some circumstances, give rise to antitrust concerns. This Code contains a separate section entitled “Antitrust” that addresses this subject in detail.

3.6 Questions About and Reporting Conflicts of Interest

It is the Employee’s responsibility to disclose any transaction or relationship that reasonably could be expected to rise to an actual or perceived conflict of interest to the Compliance Team. Employees, as determined by management, must certify that they do not have any conflicts, or have obtained the necessary approvals for certain relationships, in the annual certification process required by the Company’s Conflict of Interest policy.

3.7 Prohibition of Conflicts of Interest by Vice Presidents and above, Officers, and members of the Company's Board of Directors

An officer of the Company, an Employee with the position of vice president or above, or director of the Company (together, "Certifying Employees") shall not assume or maintain a financial interest in or relationship with another person or entity that constitutes a conflict of interest. A conflict of interest exists if Certifying Employee or their spouse has an interest in, or relationship with, any person, firm or corporation that is a supplier, customer, or competitor of the Company. For purposes of this section:

- Any financial interest should not cause divided loyalty or speculation about why the Certifying Employee has the interest. Specific factors which should be evaluated are:
  - Position within the Company;
  - Relationship of the investment amount to the Certifying Employee's financial needs;
  - When and where the investment was made; and
  - The nature and extent of the relationship.

- A conflict of interest is ownership, directly or indirectly, of an interest in any corporation, partnership or other business which:
  - Conducts activities in competition with the Company;
  - Sells supplies, services or other materials to the Company;
  - Purchases the Company's products and/or services;
  - Acts as an agent or jobber for the Company;
  - Sells or leases real estate to the Company; or
  - Otherwise represents the Company in dealings with others.

- A conflict of interest also exists if a Certifying Employee:
  - Holds any position as an officer, partner or director in any such corporation, partnership, or organization;
  - Violates the Company's policy concerning offering or accepting gifts and gratuities;
  - Is in a Personal Relationship with a direct report or is in a Personal Relationship with an Employee within the Certifying Employee's line of authority;
  - Uses Company knowledge or information for personal gain; or
  - Is involved in an activity for personal gain which for any reason is in conflict with the Company's business interests or interferes with the Employee's ability to perform their job.

Based on the foregoing examples, any business relationship by Certifying Employees which may be reasonably construed to be in violation of this policy should be reported to the Compliance Team and the Chief Financial Officer.

Furthermore, an officer (other than the CEO) must receive prior approval from the Board of Directors, the CEO, or the Compliance Team before accepting a position as a director,officer or Advisory Board member with another company, whether or not it is a supplier or competitor, for profit or non-profit, while serving as an officer of the Company. The CEO must receive prior approval from the Board of Directors before accepting any such position.

This section is not intended to preclude ownership by Certifying Employees or members of their immediate family of stock in publicly owned corporations, provided such ownership does not present substantial influence on the activities of the corporations which do business with or are in competition with the Company. This section is also not intended to preclude Certifying Employees or members of their immediate family from having a direct or indirect financial interest in or relationship with any person, firm

or corporation, provided such interest does not present substantial influence on the activities of the persons, firms or corporations which do business with or are in competition with the Company. However, all such interests must be reported annually in the form referenced below.

At least annually, each Certifying Employee within the scope of this policy as designated above, shall present an executed “Conflicts of Interest Certificate” to the Chief Financial Officer or Controller, the results of which shall be summarized and presented to the Board of Directors.

4 Technology Use and Privacy

The Company provides various Technology Resources (defined below) to authorized Employees to assist them in performing their job duties for the Company. Each Employee has the responsibility to use the Company's Technology Resources in a manner that increases productivity, enhances the Company's public image, and is respectful of other Employees. There are many critical areas as outlined below and include Cybersecurity and Technology Ethics, for which more details can be found in the NTT DATA Group Code. Failure to follow Company policies and procedures regarding Technology Resources may lead to limitation or removal of access to these Resources, as well as to disciplinary measures, up to and including termination of employment.

4.1 Technology Resources

Technology Resources include all electronic devices, software, technical documentation, technical data, and means of electronic communication, including but not limited to: personal computers and workstations; laptop computers; mini and mainframe computers; computer hardware such as disk drives, flash drives, and tape drives; peripheral equipment such as printers, modems, fax machines, and copiers; computer software applications and associated files and data, including networks, systems, and software that grants access to external services, such as the Internet; electronic mail; telephones; cellular phones; pagers; PDAs and other handheld devices; and voicemail systems.

4.2 Authorization

Access to the Company's Technology Resources is within the sole discretion of the Company. Generally, Employees are given access to the Company's various Technology Resources consistent with their job functions. The Company reserves the right to limit such access by any means available to it, including revoking access altogether.

4.3 Use of Technology Resources

The Company's Technology Resources are to be used by Employees only for the purpose of conducting Company business. Employees may, however, make use of the Company's Technology Resources for the following incidental personal use so long as such use is reasonable, does not interfere with the Employee's duties, is not done for pecuniary gain, does not conflict with the Company's business, and does not violate any Company policy or procedure or any applicable law or regulation:

- To send and receive occasional personal communications, including using the telephone system to make occasional brief personal calls;
- To prepare and store incidental personal data (such as personal calendars, personal address lists, and similar incidental personal data) in a reasonable manner; and
- To access the Internet for brief personal searches and inquiries during meal times or other breaks or outside of work hours, provided that Employees adhere to all other Technology Resource usage policies.

Any incidental use must not impede or overload the performance of any of the Company's or its customers' Technology Resources.

The Company assumes no liability for loss, damage, destruction, alteration, disclosure, or misuse of any personal data or communications transmitted over or stored on the Company's Technology Resources. The Company accepts no responsibility or liability for the loss or non-delivery of any personal electronic mail or voicemail communications or any personal data stored on any Company Technology Resources or property. The Company discourages Employees from storing important personal data on the Company's Technology Resources.

4.4 Information Security and Data Privacy

The Company has an Information Security and Data Privacy Policy ("IT Data Privacy Policy") applicable to all Employees, which prescribes how Personal Information and Personal Health Information (as defined in the IT Data Privacy Policy) of Company Employees and clients should be protected and handled. It is the Company's policy to treat Personal Information and Personal Health Information of Company Employees and clients as confidential. Such Personal Information and Personal Health Information should be accessed only by those Company Employees authorized to do so in the course of their employment, and transmitted and disposed of in accordance with the IT Data Privacy Policy:
IT Information and Data Privacy

4.5 No Expectation of Privacy; Company Right of Access to Technology Resources

As a general rule, and to the fullest extent permitted by applicable law, Employees should understand that they have no right of privacy with respect to any messages or information created, maintained, or sent on the Company's Technology Resources, including personal information or messages. NTT DATA reserves all rights, to the fullest extent permitted by law, to inspect the Company's facilities, property, records and systems, including without limitation all messages sent and received and all data and information stored on the Company's Technology Resources, including the Company's e-mail system, voicemail system, and computer systems, regardless of the content. The best way to guarantee the privacy of personal information is to not store or transmit it on the Company's Technology Resources.

Consistent with applicable law, the Company may routinely monitor or examine Employee use of its Technology Resources. The Company further reserves, to the fullest extent allowed by law, the right to access, retrieve, review, intercept, read and disclose any information stored or made available on any of its Technology Resources, including Employee and Company computer files, electronic mail, voicemail, and usage information, at any time, at the Company's sole discretion. The Company also reserves to the fullest extent allowed by law the right to monitor its Technology Resources at any time in order to determine compliance with its policies, for purposes of legal proceedings, to investigate misconduct, to locate information, or for any other business purpose.

4.6 Prohibition Against Harassing, Discriminatory, Threatening, and Defamatory Use of Email

Electronic communication is generally a less formal method of communication than written memoranda. Employees must therefore take care to avoid permitting informality to deteriorate into improper use.

Under no circumstances may an Employee use the Company's Technology Resources to transmit, request and receive, or store any information that is discriminatory, harassing, threatening, indecent, or defamatory in any way, or that, in any way, violates the Company's policy against discrimination or harassment.

4.7 Prohibition Against Violating Copyright Laws

Employees may not use the Company's Technology Resources to copy, retrieve, forward, or send

copyrighted materials unless the Employee has the author's permission or is accessing a single copy only for the Employee's reference. The downloading of software, tools, or other copyright protected material from the Internet without prior, written approval from the Company's Chief Information Officer or the Chief Information Officer's designee is prohibited. Impermissibly downloading material in violation of applicable copyright laws may lead to disciplinary measures, up to and including termination of employment. The Company reserves its rights to hold the Employee personally accountable for any resulting liability or damage to the extent permitted by applicable law.

4.8 Other Prohibited Uses

Employees may not use any of the Company's Technology Resources for any illegal purpose, in violation of any Company policy, in a manner contrary to the best interests of the Company, in any way that discloses Confidential Information of the Company or third parties (as defined in Section 4.13 below), or for personal or pecuniary gain.

4.9 Passwords

Employees who use a computer or other Company-provided Technology Resource must create and then safeguard a strong password, to protect Company Resources from improper access or use by others.

Employees are responsible for all activities occurring under their user ID.

4.10 The Internet and Online Services

The Company provides authorized Employees access to online services such as the Internet. As noted earlier, the Company expects that Employees will use these services in a responsible way and for primarily business-related purposes. Unless expressly permitted by applicable law, Employees are at all times prohibited from using the Company's Technology Resources to access, download, or contribute to the following:

- Gross, indecent, or sexually oriented materials;
- Illegal drug-oriented sites;
- Gambling and game sites; or
- Job-search sites (other than in connection with Company business).

4.11 Use of Social Networking

In general, the Company respects the rights of its Employees to use social media tools (e.g., Twitter, Facebook, LinkedIn, Instagram, WhatsApp, YouTube, TikTok, Snapchat, personal websites, blogs, wikis, etc.) (together, "Social Media"). However, all Employees are expected to observe the following guidelines when creating, posting, commenting, communicating, participating, sharing, or engaging in any form of conduct with respect to Social Media, whether using the Company's Technology Resources or not:

- Follow Company policy. All Employees should adhere to the Code, and other applicable Company policies, procedures, agreements and applicable law and regulations.

- Employees are responsible for their Social Media postings. Employees are personally responsible for the content they publish on-line via Social Media. Employees may not post content on Social Media that is vulgar, obscene, hateful, discriminatory, threatening, intimidating, or knowingly or recklessly false.

- Protect the Confidential Information of the Company and of Company clients. Employees may not use Social Media to disclose Confidential Information (which includes client information disclosed to the Company, as defined in Section 4.13 below).

- Respect copyright, fair use and financial disclosure laws. An Employee may not use Company logos or trademarks or reference any of the Company's current, former, or prospective clients, teaming partners, or suppliers, in a way which suggests that the Employee is representing the Company or while engaging in Social Media activity that is unlawful or violates Company policy. Employees may not make postings that include confidential or copyrighted information (in whatever format) belonging to third parties.

- Only Authorized Company Representatives may speak for the Company. Unless specifically instructed otherwise, an Employee is not authorized to speak, write, or post on behalf of the Company, even to correct misinformation. If a member of the news media or blogger contacts an Employee about a Social Media statement that concerns the business of NTT DATA, please refer that person to Corporate Communications & Public Relations, at public.relations@nttdata.com. If an Employee makes a statement concerning or related to the Company's business on Social Media, that Employee must clearly identify themselves as a NTT DATA Employee, and include a disclaimer that the views expressed are those of the Employee and not those of NTT DATA (e.g., "the statements made on this blog are mine and do not necessarily reflect the views of NTT DATA"). Leaders in the Company have an additional responsibility when using Social Media, as, even with a disclaimer, personal statements posted on Social Media may be misunderstood as expressing NTT DATA's position. Employees should not knowingly or recklessly make false statements on Social Media about the Company, including the Company's directors, officers, Employees, clients, products, services, business relationships, and finances.

- Do not let Social Media use impact job responsibilities. Employees should make sure that use of Social Media does not interfere with performing their job responsibilities.

- Use Common Sense and Good Judgment when using Social Media. Common sense is the best guide if an Employee decides to post information on Social Media. If an Employee is unsure about whether posting a particular statement will be in accordance with this section of the Code, the Employee should contact their HR business partner or the Communications & PR department for guidance.

- This section of the Code is intended for the protection of the Company, its clients, and its Employees. The Company respects an individual's right to self-expression and opinion. This section of the Code will not be construed, applied, or interpreted in any way so as to infringe upon the rights of Employees to self-organize, form, join, or assist labor organizations, or to bargain collectively. Nothing in this section of the Code is intended to prohibit Employees from communicating in good faith about wages, hours, or other terms and conditions of their or their co-worker's employment. Employees will not be disciplined or retaliated against for exercising their rights protected under the U.S. National Labor Relations Act or other similar laws. However, violations of Company policies or actions that otherwise damage the Company's business may result in disciplinary action, up to and including termination.

4.12 Software Use License Restrictions

All software in use on the Company's Technology Resources is officially licensed software. No software is to be installed or used that has not been duly paid for and licensed appropriately for the use to which it is being put. No Employee may load any software on the Company's computers, by any means of transmission, unless authorized in advance by the Company's Chief Information Officer. Authorization for loading software onto the Company's computers will not be given until the software to be loaded has been thoroughly tested for compatibility with installed or accessed Company business systems and software is scanned for viruses. Impermissibly downloading software for use in violation of the applicable license (e.g., using a software with a private license for commercial use) may lead to disciplinary measures, up to and including termination of employment.

4.13 Confidential Information

The Company is very sensitive to the protection of trade secrets and other confidential and proprietary information of both the Company and third parties, including suppliers and customers (together "Confidential Information"). Employees are expected to use good judgment and to adhere to the highest ethical and legal standards when using or transmitting Confidential Information, whether on the Company's, a customer's, or another party's Technology Resources.

Examples of Confidential Information include, but are not limited to, non-public information, (whether written or oral) pertaining to: trade secrets; methodologies; presentations, marketing and sales plans and forecasts, discoveries, ideas and know-how; business and strategic plans; pricing information and rate structures; merger and acquisition activity; financial plans and forecasts; plans for new service offerings and products; customer lists; customer proposals; phone lists, organization charts and e-mail lists; and the personal information or personal health information (as defined by the Company's Information Security Policies or applicable law) of Company Employees, suppliers and customers.

Unauthorized copying, use, disclosure or circulation of Confidential Information is strictly prohibited. Confidential Information may only be used within the ordinary course of employment with the Company. Confidential Information should not be accessed through the Company's Technology Resources in the presence of unauthorized individuals. Similarly, Confidential Information should not be left visible or unattended. Employees should use caution when sending Confidential Information over the Internet. Employees also should verify electronic mail addresses or facsimile numbers before transmitting any messages or Confidential Information.

Any Confidential Information transmitted via the Company's Technology Resources should be marked with a confidentiality legend. Any Confidential Information that constitutes personal information or personal health information (as defined by the Company's IT DATA Privacy Policy or applicable law) of Employees or third parties must be handled, stored, transmitted, and destroyed in accordance with applicable law and the Company's IT Data Privacy Policy and its Information Security Policies.

4.14 Technology Ethics

NTT DATA Group engages in a variety of research and development activities. The new technologies that are created through such research and development activities must be able to maintain the symbiosis between humans and nature. To this end, NTT DATA Group believes that it is necessary to deepen our understanding of the characteristics of new technologies, constantly explore them, and pursue research and development activities, utilization, and implementation of new technologies to society with high ethical standards such as respect for human rights and consideration for nature.

In particular, Artificial Intelligence (AI) will become more prevalent in society and will affect people's behavior and decision-making. For the purpose of reducing the number of negative incidents potentially arising from AI, and realizing a human-centered society in which humans and AI truly coexist, NTT DATA Group, as a position to promote research, development, operation, and utilization of AI, will promote the development activities and application of AI technology to business in accordance with applicable laws and regulations, as well as NTT DATA Group's AI Guidelines.

In accordance with NTT DATA Group's AI Guidelines, we will promote innovation through dialogue and collaborations with diverse stakeholders by realizing fair and trustworthy AI, while preventing potential discrimination and use of biased data and giving due consideration to privacy and security.

* For details: NTT DATA Group's AI Guidelines:
https://www.nttdata.com/global/en/About%20Us/AI%20Guidelines

5 Gifts, Gratuities, Entertainment, and Other Considerations

5.1 Gifts

Except as set out below, Employees should refrain from giving and receiving business-related gifts. Any exceptions to this guideline must be approved in writing by the Compliance Team.

5.1.1 Receiving Gifts.

No Employee may solicit any business-related gift, or accept any gift or gifts worth more than

$250 over the course of a calendar year, from a person or organization seeking to have or who has a business relationship with the Company, or has interests that could be substantially affected by actions of the Company.

5.1.2 Giving Gifts.

No Employee may give, offer or promise a business-related gift or gifts worth more than $250 over the course of a calendar year to any person or organization on behalf of the Company.

Note that the rules on this topic relating to U.S. and foreign government personnel are stricter. See Section 5.3 below.

No Employee may give, offer or promise a gift of any value to any person or organization where it could reasonably be interpreted that the purpose of the gift was to induce improper performance or to obtain or retain business, or an advantage in the conduct of business, for the Company.

No Employee should accept a customer, vendor, or supplier discount for themselves unless it is made available to all Company Employees or otherwise approved by the Compliance Team.

Invitations to participate in so-called “directed shares,” “friends and family,” and similar stock purchase programs of customers, vendors, or suppliers of the Company are considered to be gifts. Employees should decline to participate in such programs unless they have sought and received written approval to participate from the appropriate Division Leader and the Compliance Team. Such approval may be granted where the offer to participate was made to the Employee irrespective of any past, present, or future connection with the Company and without the actual or apparent intent to influence the Employee’s objective business judgment.

5.2 Business-related Meals, Entertainment, and Travel

Employees may provide or accept business meals, entertainment, lodging, and travel, including attendance at sporting or cultural events, as long as it: (1) is associated with an occasion at which business is discussed; (2) is professionally appropriate; and (3) and is provided as a normal part of business, and could not reasonably be interpreted as being for the purpose of inducing performance or obtaining or retaining business, or an advantage in the conduct of business, for the Company.

The value of the activity must be reasonable and permissible under the Company’s expense account procedures, regardless of whether or not the Company is paying for the activity. Except for attendance at NTT DATA Corporate-sponsored hospitality events, Employees must obtain prior, written approval from their leader before accepting or offering business-related lodging, travel, or attendance at sporting, cultural, or other business entertainment events the value of which exceeds $250.

5.3 Gifts and Entertainment Rules with Respect to Government Officials and Employees

The laws and rules concerning doing business with governments and their officials and employees are complex and very restrictive. Many countries have laws that significantly limit or prohibit the ability of government officials or employees to give or accept gifts or business entertainment or meals.

With this in mind, Employees may not give or offer to give to any government employees or officials who are prohibited from accepting such consideration any entertainment, meal, travel, gift, or other item of value.

If government employees or officials are present at conferences or meetings at which the Company is providing refreshments or a light meal, a contribution basket should be placed conspicuously next to the refreshments so that the government employees and officials may contribute an appropriate amount for the cost of any refreshments or meals they consume.

For a further explanation of guidelines applicable to doing business with the government, see section 8.1, entitled “Government Contracting”, in this Code.

5.4 Bribes and Kickbacks

Paying, or offering to pay, a bribe or a kickback to anyone, for any reason, by any means, is strictly prohibited. Likewise, Employees may not solicit, agree to receive or accept a kickback or bribe, in any form, for any reason.

This is not limited to cash or other monetary payments. It includes any financial or other advantage. A “financial or other advantage” includes, but is not limited to, money, favors, entertainment, or gifts.

For more information on this topic, please see the Global Anti-Corruption and Bribery Policy.

6 Business Relationships

6.1 Customer Relationships

The Company's customers are of the utmost importance to the Company. Employees should always treat customers and potential customers ethically and according to the highest standards of business conduct.

It is the Company's policy to always sell its products and services on their merits and to avoid making disparaging comments about the products and services of competitors. Employees should refrain from commenting upon the character, financial condition, or potential legal or regulatory problems of competitors. Employees should follow the following guidelines in selling the Company's products and services:

- Sell on the strength of the Company and its services and products, not on the weaknesses of its competitors.
- Do not make claims about the Company's products or services unless the claims are both factual and complete and can be fully substantiated.
- Do not make claims about a competitor's products or services unless the claims are based on the competitor's current published materials or other factual data approved for selling purposes by the Company.
- If a customer or potential customer has a contract with a competitor or has placed a firm order with a competitor, do not suggest or imply in any way that the customer revoke, rescind or breach that contract or order.

6.2 Privacy of Customer Communications

The Company's customers trust us with one of their most important assets — information. We must honor this trust by protecting the privacy of customer communications, whether the communication is in electronic, voice, written, or other form.

The Company has established the following guidelines to protect privacy of customer communications:

- Do not eavesdrop on, record, or divulge the contents of any customer conversation, electronic message, document, or other transmission. Never let anyone else do so.
- Do not divulge to any other individual, except an authorized Employee requiring the information for a legitimate business reason, any information about the customer's (or their customers') communications, identity, or other business information or records.
- Do not use any customer information from any non-public source for personal benefit or that of anyone else.
- Do not access customer records or information in any system, for any reason, except for official Company business.

6.3 Selecting Suppliers

The Company's suppliers — companies and individuals that sell products and services to the Company — are vital to our business. Employees should always treat suppliers and potential suppliers ethically and in accordance with the highest standards of business conduct.

Suppliers should be selected on the basis of objective criteria, such as value (quality for price), price, technical excellence, service reputation, and production/service capacity. Employees should never say, sign or write anything that a supplier or potential supplier may reasonably interpret as a commitment to do business unless expressly authorized to do so.

Suppliers must adhere to NTT DATA's Third-Party Global Code of Business Conduct and Supplier Standards.

6.4 Working with Existing Suppliers

Employees should comply with the following rules when working with existing suppliers, which includes NTT Group companies that are not within the NTT DATA family:

- Never interfere with a supplier's contracts or business relations with a competitor of the Company.
- Never reveal Confidential Information about one supplier to another supplier or to anyone outside of the Company. This includes confidential or non-public information about services or products supplied, pricing, service level assurances, purchase volumes, and other terms and conditions.
- Follow the Company's guidelines concerning gifts, gratuities, entertainment, and other considerations of value. Section 5 of this Code, entitled "Gifts, Gratuities, Entertainment, and Other Considerations", discusses this subject in greater detail.
- Avoid any interest that conflicts with, or appears to conflict with, their or another Employee's responsibility to the Company. Section 3 of this Code, entitled "Conflicts of Interest", discusses this subject in greater detail.
- Reject any agreement with a supplier that restrains, or may appear to restrain, competition. Such agreements violate Company policy and may violate the law. Employees with procurement responsibility should review the sections of this Code concerning government contracting and antitrust and should be familiar with applicable laws. If an Employee is unsure whether a proposed agreement violates this guideline, contact the Compliance Team.

6.5 Sales Agents, Representatives, Distributors, and Consultants

Agreements with sales representatives, agents, marketing consultants, distributors, and other parties require adherence to Company policies and applicable U.S. and foreign government laws and regulations. The Company requires appropriate management approval (including, but not limited to, appropriate contract and signature approval policies) and review by the Corporate Legal Department prior to entering into any such agreements.

Employees should take the necessary steps to ensure that the Company's intermediaries, consultants, distributors, agents, and representatives are familiar with, understand, and adhere to the applicable policies contained in this Code.

6.6 Contracts and Commitments

No Employee may agree to or sign any document, contract or agreement binding the Company without express authorization by an authorized Company Employee.

The Company has instituted contract and signature approval policies that identify those Employees who have authority to approve and sign certain contracts binding the Company. If there are any questions about which Employees have signature authority for a given contract, contact the Corporate Legal Department. In addition, there are policies governing which suppliers the Company may use. All supplier contracts should be reviewed by Procurement.

An Employee should never say or write anything — including, for example, entering into a letter of intent, memorandum of understanding, letter agreement, or side letter — that could be construed by another party as a commitment by the Company, unless expressly authorized to do so. Any questions about what constitutes a legal commitment should be directed to the Compliance Team.

7 Doing Business Globally

The Company is committed to the highest business conduct standards wherever it operates. The Company observes these standards worldwide, even at the risk of losing business. While no one can anticipate all the situations that may present challenges to Employees doing business in the worldwide marketplace, the following guidelines always apply:

- Observe all laws and regulations, both U.S. and non-U.S., that apply to our business abroad.
- Paying bribes to government officials or to their immediate family members is absolutely prohibited, even if those bribes are common practice. Employees may not give, promise to give, or authorize giving to a foreign official, a foreign political party, an official of a foreign political party, a candidate for foreign political office, or to any international organization, any money, gift, or anything of value to: (1) influence their acts or decisions; (2) induce them to do or omit to do any act in violation of their lawful duty; or (3) induce them to use influence with a foreign government or agency.
- Paying bribes to third parties anywhere in the world (whether the third party is a public official, a private individual or an incorporated or unincorporated organization) is absolutely prohibited. Employees and agents of the Company must comply with Section 5.4 of this Code ("Bribes and Kickbacks") and the Global Anti-Bribery and Corruption Policy irrespective of where they are conducting business.
- Do not cooperate with illegal boycotts.
- Observe all licensing requirements and the requirements of applicable import and export control laws, as well as all laws and regulations pertaining to privacy and data transfer.
- Do not enter into an agreement with an agent or consultant that relates to the Company's business outside the United States unless all appropriate approvals have been obtained as set forth in the Company's policies and the policies of its foreign affiliates and subsidiaries (including applicable matrix/approval policies).
- The laws governing the Company's business in foreign countries are extensive and complex and may be different from those in the United States. No new Company services should be offered in any new country without the prior approval of the Corporate Legal Department and then only in accordance with the local country's applicable regulations and requirements.

If an Employee has any questions about the legality of providing Company services in any country or about any aspect of law or regulation, contact the Corporate Legal Department.

7.1 No Payments to Low-Level Non-U.S. Governmental Employees and Officials

U.S. law permits certain "facilitating" payments to obtain or expedite the performance of commonly performed, routine, nondiscretionary government action by a foreign government official (note that facilitating payments to U.S. officials are not permitted). Examples of facilitating payments include obtaining official documents to qualify a person to conduct business; processing government papers such as visas and work orders; providing police protection, mail service, and phone service; and loading and unloading cargo.

The Company adopts a zero-tolerance approach to facilitating payments. Any facilitating payments made by Employees or agents, except in the emergency circumstances outlined below, is a violation of this Code.

Employees or agents are only permitted to make a facilitating payment in circumstances where they are exposed to an immediate threat of loss of life, limb, or liberty. Once the immediacy of the situation has been resolved, the matter should be reported to the Compliance Team and fully and accurately recorded on the Company's books.

If there are questions regarding the reporting of facilitating payments, contact the Corporate Legal Department or a member of the Compliance Team.

7.2 Export Regulation

Because of the international nature of our business, the Company is subject to the export laws and regulations of numerous countries. These laws and regulations govern the international transfer of all products and services of the Company, as well as technology, information and ideas belonging to the Company.

Under United States law, no Technology (defined below), including, without limitation, the Company's and its customers' and suppliers', may be exported without the proper government export licenses and documentation.

Exports of Technology include not only Technology shipped via freight, but also Technology that is hand-carried (Employees traveling overseas), sent via courier services or United States mail, electronically transmitted, or disclosed to foreign nationals in the United States or abroad. "Technology" is defined as hardware, software, technical documentation, product specifications, and technical data.

It is the responsibility of Employees to ensure that proper documentation accompanies each export or disclosure. Any export or re-export without the proper export license or documentation can jeopardize the Company's compliance with applicable export laws. Non-compliance can result in denial of export privileges, criminal penalties, seizure of commodities, and/or fines to the Company and its Employees.

Any questions regarding this policy or an export in particular should be directed to the Compliance Team.

7.3 Anti-Boycott

The United States has enacted anti-boycott regulations which make unlawful certain actions, including but not limited to furnishing information about business relationships with boycotted countries, or information about race, religion, sex, or national origin.

Anti-boycott compliance issues arise most frequently in connection with the Arab boycott of Israel. In the event that an Employee or Company agent is asked for any prohibited information or to take any action in furtherance of a boycott, the Employee or agent should respond only with the following statement: "Company policy and United States law do not permit me to respond" to the question or request.

Requests for boycott information, or requests to take any actions in furtherance of a boycott, must be reported immediately to the Compliance Team.

8 The Government, Securities Laws and the Media

8.1 Government Contracting

The Company is committed to conducting business in accordance with all applicable laws and regulations and with the highest ethical standards. Detailed laws and regulations govern virtually every aspect of doing business with a country's government and their provincial, state, and local governments and agencies. Employees must adhere to the highest standards of honesty and integrity in their relations with government officials and employees, including, without limitation, observing the following principles when disclosing information related to, bidding on, or performing under government contracts:

- Comply with the requirements of all applicable government acquisition regulations, including, with respect to the US Government, the Armed Services Procurement Act, the False Claims Act (FCA), the Federal Acquisition Regulation, the Procurement Integrity Act, the Truth in Negotiations Act, and all agency-specific acquisition regulation, cost principles, and Cost Accounting Standards. For example, Employees should refrain from engaging in any conduct that could be deemed to violate the FCA or otherwise mislead the US Government or any higher tier prime contractor.

- In addition, Employees should: (1) ensure that their time is properly recorded, (2) verify that each invoice for which they are responsible lists the correct product or service, quantity, and price; (2) ensure that products and services comply with applicable contract requirements, including appropriate signature approvals; (3) refrain from making any representation, certification, or statement unless it is known and approved by the Corporate Legal Department and known for certain to be true; and (4) immediately report to the Corporate Legal Department or the Compliance Team any actual or suspected violation of the FCA or any other government regulation.

- Without limiting the generality of the above paragraph, no Employee or agent of the Company may engage in prohibited discussions, offer gratuities, or solicit or receive proprietary or source selection information from a government procurement official. No Employee or agent of the Company may subject themselves or the Company to civil or criminal penalties by presenting false claims or false statements to an agency or agent of a government.

- Do not offer or provide meals, transportation, gifts, or other consideration to any government employees who are prohibited from receiving such consideration. If government employees or representatives are present at conferences or meetings at which the Company is providing refreshments or a light meal, a contribution basket should be placed conspicuously next to the refreshments so that the government employees or representatives may contribute an appropriate amount for the cost of any refreshments or meals they consume.

- Obey all government election requirements and adhere to Company practices and policies related to such requirements (including, without limitation, those listed in Section 8.4 of this Code) concerning political contributions and any limitations, including reporting requirements, on gifts and travel imposed by government legislatures.

- Obey the regulations concerning the employment of (or discussions concerning possible employment with) current and former officials and employees of governmental agencies, including so-called "revolving door" restrictions. Obtain all appropriate government approvals prior to recruiting or hiring current and former government employees.

- Obey all export regulations and obtain appropriate licenses prior to exporting or even discussing government customer data and technologies with citizens of other countries, even if they are located in the country where the Employee is located. With respect to activities occurring in the United States,

Employees should comply with all applicable requirements of the Export Administration Regulation and the International Traffic in Arms Regulation.

- Adequately safeguard sensitive and classified information belonging to government customers in accordance with the Company's and its subsidiaries' security agreements, practices and policies and do not disclose such information, even to Employees of Company affiliates, except in accordance with applicable government security regulations and as expressly authorized by Company directives and policies.

- Complete in accordance with Company policies and instructions all ethics training curriculum that is required by the Company to be completed and made available to Employees.

These guidelines are not intended to be all-inclusive, and Employees who deal with the government or work on matters relating to government contracts should familiarize themselves with the Company's (including, for the avoidance of doubt, its subsidiaries') security agreements, practices and policies on interacting and contracting with government employees, representatives and agencies.

Employees who deal with government employees, representatives and agencies are responsible for knowing and obeying the laws and regulations applicable to doing business with the government.

Questions relating to these laws, regulations, or any other aspect of doing business with the government should be referred to the Compliance Team.

8.2 Inside Information and the Laws Against Insider Trading

Inside information is material information about a publicly traded company that is not known by the public. Information is considered "material" if it could affect the market price of a security or if a reasonable investor would attach importance to the information in deciding whether to buy, sell, or hold a security.

Inside information often relates to financial conditions, such as progress toward achieving revenue and earnings targets or projections of future earnings or losses of any company. Inside information also includes changes in strategy regarding a proposed merger, acquisition or tender offer, new products or services, contract awards, and other similar information.

Inside information is not limited to information about the Company. It also includes material, non-public information about others, including the Company's customers, suppliers, competitors, and shareholders.

Insider trading occurs when an individual with material, non-public information trades securities or communicates such information to others who trade. An insider who trades on the basis of material inside information violates the law. An insider who "tips" others violates the law if such person's trade on the basis of material inside information. For purposes of this policy, "Insider" means all officers, directors, Employees, consultants, and contractors of the Company and its subsidiaries, and all members of the immediate families and households of those persons. In addition, anyone who receives inside information from an Insider is an Insider. Insiders should assume that they have material inside information about customers or suppliers.

Insiders are prohibited from:

- Buying or selling stock or other securities while aware of inside information.

- Passing inside information to others, including Family Members.

- Trading when in possession of inside information received because of a confidential relationship or permitting others to trade on the information.

- Trading in the securities of other companies, including the securities of the Company's customers or vendors, when in possession of inside information relating to such other companies.

Trading or helping others trade while aware of inside information has serious legal consequences, even if the Employee does not receive any personal financial benefit. Employees may also have an obligation to take appropriate steps to prevent insider trading by others. Any insider possessing inside information may not discuss or disclose such information with or to any other Employee or outside contact, unless that individual has a clear right or need to know such information in order to fulfill their responsibilities to the Company.

Under no circumstances should an insider make inside information available to their Family Members or business or social acquaintances. The responsibility to safeguard against improper use of insider information cannot be evaded by acting indirectly through another person.

U.S. federal law imposes severe sanctions against those who engage in insider trading. Individuals who trade on inside information may be subject to: (1) criminal fines of up to $1,000,000; (2) prison sentence of up to ten years; and (3) civil penalties of up to three times the profit gained or loss avoided as a result of such sale, purchase or communication. Any Employee of the Company who violates this policy will be subject to disciplinary action. In addition, Employees of the Company are responsible for ensuring that their Family Members comply with this policy. Any failure to do so may result in disciplinary action.

8.3 Antitrust

Antitrust rules limit what companies can do with other companies and what companies can do on their own. Generally, the antitrust laws are designed to prohibit agreements or actions that reduce competition and harm consumers. Under no circumstances may an Employee enter into an agreement, or discuss entering into an agreement, with a competitor that restricts competition by fixing or controlling prices, rigging bids, dividing and allocating markets, territories, or customers, boycotting suppliers or customers, or by any other means. United States and foreign antitrust laws also apply to imports and exports.

Additionally, Employees should not engage in the following specific activities without prior approval from the Compliance Team:

- Sharing marketing plans or business policy matters.
- Submitting a joint bid or "teaming" with another company on projects.
- Working with competitors to establish industry-wide standards.
- Requiring a customer to buy one product or service from the Company in order to be able to buy a second product or service from the Company.
- Requiring a customer to buy products or services only from the Company and not from a competitor.
- Requesting a supplier to buy from the Company in exchange for the Company buying from the supplier.
- Agreeing with a customer or supplier on the price or other terms on which a product or service can be resold.
- Refusing to deal with someone who wants to buy Company products or services or cutting off someone who already buys them.
- Refusing to buy from a supplier that deals with one of the Company's competitors.

- Trying to persuade a customer or supplier, or any other person to do business with the Company and to stop doing business with a competitor with whom it has a contract or continuing business relationship.

Any questions regarding these activities or requests for an exception to these rules should be directed to the Compliance Team.

8.4 Political Contributions

No political contributions are to be made using Company funds or assets, or the funds or assets of any Company subsidiary, to any political party, political campaign, political candidate, or public official in the United States or any other country, unless the contribution is lawful and expressly authorized in writing by the Company's Chief Financial Officer and Corporate Legal Department. In addition, no Employee may make a political contribution on behalf of the Company or its subsidiaries, or with the appearance that such contribution is being made on behalf of the Company or its subsidiaries, unless expressly authorized in writing by the Company's Chief Financial Officer and Corporate Legal Department.

Nothing in this policy is intended to discourage Employees from making contributions of their own time and/or funds to political parties or candidates of their choice. However, Employees will not be compensated or reimbursed by the Company for any personal contributions.

Rules and laws concerning United States political action committees ("PACs") govern contributions to and by PACs. In the event the Company permits the formation of one or more PACs, Employees must comply with all rules and laws applicable to contributing to those organizations.

9 Accuracy of Reports

The Company will comply with all applicable reporting requirements and regulations wherever the Company does business. All Employees and leaders are responsible for the accuracy of the records, time sheets, and reports they work on, submit, or approve. Accurate information is essential to the Company's ability to meet legal and regulatory obligations and to compete effectively. The records and books of account of the Company shall meet the highest standards and accurately reflect the true nature of the transactions they record.

No undisclosed or unrecorded account or fund shall be established for any reason. Employees may not create any false or misleading documents or accounting, financial, or electronic records for any purpose, and no one may direct Employees to do so. For example, expense reports must accurately document expenses actually incurred in accordance with Company policies. Employees must not obtain or create "false" invoices or other misleading documents or records, or invent or use fictitious entities, sales, purchases, timesheets, services, loans or other financial arrangements for any purpose. All invoices issued to customers must accurately reflect the product sold or service rendered. Invoices must be based upon the true and agreed upon sales price and terms of sale, even when a customer may request something different.

Similarly, Employees who report their work time are responsible for accurately reporting time worked on the Company's authorized time keeping system and within the time periods specified in the Company's procedures and policies (e.g., Time Compliance and Reporting Policy US/Canada/India & ROW).

If there are any questions, or if an Employee feels they are being asked to create a document or an electronic record in a less than complete, honest, and accurate manner, the Employee must immediately report this to their leader, the Corporate Legal Department, the Compliance Team, Internal Audit, or the Ethics Hotline.

10 Concerns Regarding Accounting, Auditing, Fraud, Money Laundering or Internal Control Matters

The financial statements of the Company shall conform to generally accepted accounting principles and the Company's accounting policies.

The Company is committed to and requires strict conformance to the taxing and other financial reporting requirements of all jurisdictions where it does business. The Company likewise takes seriously its obligation to minimize the risk of fraud and other financial misconduct, including money laundering.

Anyone with concerns or complaints regarding accounting, internal controls, fraud, financial misconduct, money laundering or auditing matters may confidentially submit such concerns or complaints to Internal Audit, the Compliance Team, or by calling the toll-free Ethics Hotline. Any such concerns also may be reported anonymously where permitted by local law. The matter will be investigated, and appropriate action taken.

The Company will not discipline, discriminate against or retaliate against any Employee who reports a complaint or concern (unless the Employee is found to have knowingly and willfully made a false report).

11 Compliance and Reporting

11.1 Reporting Procedures and Other Inquiries

Anyone having knowledge of, or questions or concerns about, an actual or possible violation of the provisions of this Code must immediately report the matter to their immediate leader or via one of the options below.

- Online via the "Report Online" portal: https://nttdata.i-sight.com/landing-page
- By phone: Continental US and Canada dial 1-855-399-6120 and in Mexico dial 1-800-522-6497.
- For a list of phone numbers for other locations reference the "Report Online" portal at https://nttdata.i-sight.com/landing-page
- The Compliance Team, via the "Report Online" portal: https://nttdata.i-sight.com/landing-page
- The Employee Relations CoE
- The HR Business Partner assigned to their team
- Internal Audit

11.2 Investigations

Employees have an obligation to cooperate fully, truthfully, and candidly with all Company investigations of alleged violations of this Code or other company policies. Failure to cooperate or to be truthful in an investigation may lead to discipline up to and including termination, consistent with local law.

Retaliation against anyone who makes a good faith complaint of improper conduct, or who cooperates with an investigation into such conduct, will not be tolerated.

Investigations into alleged violations of this Code or any Company policy may be conducted by one or more members of the Compliance Team, HR, Internal Audit, and others, including outside counsel or other third parties.

11.3 Discipline

Any Employee who violates the provisions of this Code will be subject to disciplinary action, up to and including termination.

In addition, any Employee who retaliates against someone for reporting a potential violation in good faith, or for participating in an investigation in good faith, may face disciplinary action, up to and including termination.

11.4 Waivers to Sections of the Global Code of Business Conduct

While some of the policies contained in the Code must be strictly adhered to and no exceptions can be allowed, in some cases exceptions may be possible. Any Employee who believes that an exception to any of these policies is appropriate should discuss an exemption with their leader. If the leader agrees that an exemption is appropriate, the approval of the appropriate Division Leader and the Compliance Team must be obtained.

11.5 The Compliance Team

Sheri Bowman
Senior Director, Employee Relations
(703) 848-7309
sheri.bowman@nttdata.com

Meg Dholabhai
VP and Head of Internal Audit and ERM
(214) 425-7967
meg.dholabhai@nttdata.com

Stephanie Liebman
SVP, Finance
(469) 535-2770
stephanie.liebman@nttdata.com

Scot McDonald
SVP, Finance Administration
(972) 624-7928
scot.mcdonald@nttdata.com

Chelsea Teachout
VP, Legal
(917) 202-8081
chelsea.teachout@nttdata.com

12 Summary

This Code states the Company's general policy. It does not and cannot cover all situations that may confront Employees.

All Employees are expected to obey the law and to conduct their business relationships in a fair, open, and honest manner. Applying the principles in this Code requires common sense and good judgment. Employees are encouraged to review this Code periodically, to think about it, and to make sure that every aspect of their daily business life conforms to the standards it sets. If there are questions, either about these guidelines or about other Company policies, Employees are encouraged to discuss them with their leader, Human Resources, the Compliance Team or the Corporate Legal Department.