Virtusa Corporation
Code of Business Conduct and Ethics – Chief Executive Officer's Message
February 25, 2025

Dear Fellow Employees and Directors:

You will find our Code of Business Conduct and Ethics in the booklet included with this letter. Our Code is not just a reaffirmation of the Company's commitment to conducting its business ethically and to observing applicable laws, rules and regulations, it is an extension of our values and the way we do business.

The reputation and continued success of Virtusa Corporation is dependent upon the conduct of its directors, employees, contractors and agents, which conduct includes upholding our core values of passion, innovation, respect, and leadership ("PIRL"). Each of us is a custodian of the Company's good name and has a personal responsibility to ensure that her or his conduct protects and promotes both the letter of the Code and its spirit of ethical conduct. Our adherence to these ethical principles, including PIRL, is fundamental to our continued and future success, reputation, and brand.

The Code cannot provide definitive answers to all questions. Accordingly, the Company expects each individual to exercise reasonable judgment to determine whether a course of action is consistent with the Company's ethical standards and to seek guidance when appropriate. Your manager or human resource business partner will often be the person who can provide you with thoughtful, practical guidance in your day- to-day duties. We have also appointed our General Counsel, Paul D. Tutun, as our Compliance Officer, so you should feel free to ask questions or seek guidance from Mr. Tutun.

Please read the Code carefully. If you have any questions concerning the Code, please speak with your manager, human resource business partner or the Compliance Officer. Senior officers, directors and certain other employees or personnel will also be asked from time to time by the Company to confirm to the Company annually that they have read, understood and complied with the Code.

I entrust these principles and policies to you. Please give them your thoughtful and frequent attention. Please join me in making the commitment to uphold the Code.

Sincerely,

Nitesh Banga
President and Chief Executive Officer
Sensitivity: General

VIRTUSA CORPORATION
Code of Business Conduct and Ethics
Introduction

Purpose and Scope:

The Board of Directors of Virtusa Corporation (together with its subsidiaries and affiliates, the ("Company") has established this Code of Business Conduct and Ethics to aid the Company's directors, officers and employees in making ethical and legal decisions when conducting the Company's business and performing their respective day-to-day duties. The Code extends to all employees of the Company (including those of its subsidiaries), regardless of when such person was hired or became associated with the Company as well as all contractors, personnel and agents, both within and outside the United States.

The Company's Board of Directors, or a committee of the Board, is responsible for administering the Code. The Board of Directors has delegated day-to-day responsibility for administering and interpreting the Code to a Compliance Officer. Our General Counsel has been appointed the Company's Compliance Officer under this Code.

The Company expects its directors, officers and employees to exercise reasonable judgment when conducting the Company's business. The Company encourages its directors, officers and employees to refer to this Code frequently to ensure that they are acting within both the letter and the spirit of this Code. The Company also understands that this Code will not contain the answer to every situation you may encounter or every concern you may have about conducting the Company's business ethically and legally. In these situations, or if you otherwise have questions or concerns about this Code, the Company encourages each officer and employee to speak with his or her supervisor (if applicable) or with the Compliance Officer under this Code. If you have any questions or concerns about this Code and you are a director of the Company, you should speak with the Board of Directors through its Chairman, or a committee thereof responsible for administering and interpreting this Code.

Contents of this Code:

This Code has two sections which follow this Introduction. The first section, "***Standards of Conduct,***" contains the actual guidelines that our directors, officers and employees are expected to adhere to in the conduct of the Company's business. The second section, "***Compliance Procedures,***" contains specific information about how this Code functions including who administers the Code, who can provide guidance under the Code, and how violations may be reported, investigated and disciplined. This second section also contains a discussion about waivers of and amendments to this Code.

A Note About Other Obligations

The Company's directors, officers and employees generally have other legal and contractual obligations to the Company. This Code is not intended to reduce or limit the other obligations that you may have to the Company. In particular, each director, officer and employee is subject to the Company's Policy on Insider Trading and Disclosure, and employees are subject to the Company's Employee Handbook. Instead, the standards in this Code should be viewed as the minimum standards that the Company expects from its directors, officers and employees in the conduct of its business.

Standards of Conduct

Conflicts of Interest

The Company recognizes and respects the right of its directors, officers and employees to engage in outside activities that they may deem proper and desirable, provided that these activities do not impair or interfere with the performance of their duties to the Company or their ability to act in the Company's best interests. In most, if not all, cases this will mean that our directors, officers and employees must avoid situations that present a potential or actual conflict between their personal interests and the Company's interests.

A "conflict of interest" occurs when a director's, officer's or employee's personal interest interferes with the Company's interests. Conflicts of interest may arise in many situations, including the following:

- *Outside Employment and Other Affiliations. A conflict of interest may arise if an individual is simultaneously employed or engaged by the Company and another business concern, particularly a Company customer or business partner.*

- *Activities with Competitors. A conflict of interest arises if an individual takes part in any activity that enhances or supports a competitor's position, including accepting simultaneous employment with a competitor.*

- *Gifts. While entertaining customers in the ordinary course of business is not prohibited, a conflict of interest may arise if an individual or any member of an individual's immediate family gives or accepts any gift with the intent to improperly influence the normal business relationship between the Company and its customers or other business partners or gives or accepts any lavish gifts from a competitor.*

- *Investments in Other Businesses. A conflict of interest may arise if an individual or any member of an individual's immediate family holds a financial interest in an outside business concern, particularly, a Company customer or business partner. Many factors must be considered in determining whether a conflict of interest exists in this situation, including the size and nature of the investment; the ability to influence the Company's decisions that could affect the outside business concern; access to confidential information of the Company or of the outside business concern; and the nature of the relationship between the Company and the outside business concern.*

- *Conducting Business with Family Members. A conflict of interest may arise if an individual conducts business on behalf of the Company with a business in which a family member, including siblings, step-parents and step-children, of such individual or such individual's spouse, or person sharing the same household with such individual, is associated in any significant role. The Compliance Officer must be informed of all situations in which the Company is conducting business with any member of an employee's family or person sharing the same household as the employee.*

Each individual's situation is different and in evaluating his or her own situation, a director, officer or employee will have to consider many factors. Each employee is responsible for promptly reporting to the Compliance Officer any transaction or relationship that reasonably could be expected to give rise to a conflict of interest. The Compliance Officer may notify the Board of Directors or a committee thereof or take other action as he or she deems appropriate. Actual or potential conflicts of interest involving a director or executive officer should be disclosed directly to the Chairman of the Board of Directors or a committee thereof responsible for administering this Code.

Compliance with Laws, Rules and Regulations

The Company seeks to conduct its business in compliance with both the letter and the spirit of applicable laws, rules and regulations, including but not limited to the CFA 2017 (detailed below). We expect all of our employees to have a sound knowledge of the proper and improper courses of conduct both with regard to their own activities and those with whom they must deal. We also expect employees to be familiar with the material laws and regulations applicable to business activities in their territory. No director, officer or employee shall engage in any unlawful activity in conducting the Company's business or in performing his or her day-to-day company duties, nor shall any director, officer or employee instruct others to do so.

This Code and the compliance with this Code may be subject to the applicable local laws, rules, and regulations of non-U.S. jurisdictions. Accordingly, if there is a conflict between the requirements of the laws applicable in the United States and those of any other country or jurisdiction which may be relevant in the circumstances, the Company's policy is that Company personnel should consult with the Compliance Officer before taking any action that may be unlawful under, or violate, any such laws.

Protection and Proper Use of the Company's Assets

Loss, theft and misuse of the Company's assets have a direct impact on the Company's business and its profitability. Directors, officers and employees are expected to protect the Company's assets that are entrusted to them and to protect the Company's assets in general. Directors, officers and employees are also expected to take steps to ensure that the Company's assets are used only for legitimate business purposes.

Corporate Opportunities

Directors, officers and employees owe a duty to the Company to advance its legitimate business interests when the opportunity to do so arises. Each director, officer and employee is prohibited from:

- diverting to himself or herself or to others any opportunities that are discovered through the use of the Company's property or information or as a result of his or her position with the Company unless such opportunity has first been presented to, and rejected by, the Company
- using the Company's property or information or his or her position for improper personal gain, or
- Competing with the Company.

Confidentiality

Confidential information generated and gathered in the Company's business plays a vital role in its business, prospects and ability to compete. "Confidential information" includes all non-public information that might be of use to competitors or harmful to the Company or its customers if disclosed. Directors, officers and employees may not disclose or distribute the Company's confidential information, except when disclosure is authorized in writing by the Company or required by applicable law, rule or regulation or pursuant to an applicable legal proceeding. Directors, officers and employees shall use confidential information solely for legitimate company purposes. Directors, officers and employees must return all of the Company's confidential and/or proprietary information in their possession to the Company when they cease to be employed by or to otherwise serve the Company.

Fair Dealing:

Competing vigorously, yet lawfully, with competitors and establishing advantageous, but fair, business relationships with customers and suppliers is a part of the foundation for long-term success. However, unlawful and unethical conduct, which may lead to short-term gains, may damage a company's reputation and long-term business prospects. Accordingly, it is the Company's policy that directors, officers and employees must endeavor to deal ethically and lawfully with the Company's customers, suppliers, competitors and employees in all business dealings on the Company's behalf. No director, officer or employee should take unfair advantage of another person in business dealings on the Company's behalf through the abuse of privileged or confidential information or through improper manipulation, concealment or misrepresentation of material facts.

Accuracy of Records

The integrity, reliability and accuracy in all material respects of the Company's books, records and financial statements is fundamental to the Company's continued and future business success. No director, officer or employee may cause the Company to enter into a transaction with the intent to document or record it in a deceptive or unlawful manner. In addition, no director, officer or employee may create any false or artificial documentation or book entry for any transaction entered into by the Company. Similarly, officers and employees who have responsibility for accounting and financial reporting matters have a responsibility to accurately record all funds, assets and transactions on the Company's books and records.

Political Contributions

Business contributions to political campaigns are strictly regulated by U.S. federal, state and local law. Accordingly, all political contributions proposed to be made with the Company's funds must be coordinated through and approved by the Compliance Officer. Directors, officers and employees may not, without the approval of the Compliance Officer, use any of the Company's funds for political contributions of any kind to any political candidate or holder of any national, state or local government office. Directors, officers and employees may make personal contributions, but should not represent that he or she is making any such contribution on the Company's behalf. Similar restrictions on political contributions may apply in other countries. Specific questions should be directed to the Compliance Officer.

Entertaining or Doing Business with the United States and Foreign Governments; Anti- Bribery and Corruption

Giving anything of value to a government employee for the purpose of obtaining or retaining business is strictly regulated and in many cases prohibited by law. The Company and its directors, officers and employees must also comply with U.S. federal, state and local laws, as well as foreign government laws, governing the acceptance of business courtesies. Directors, officers and employees must refrain from giving anything of value to U.S. federal, state and local government employees with whom the Company does business, except promotional items of little intrinsic value and modest refreshments. In addition, directors, officers and employees should consult with the Compliance Officer before giving anything of more than nominal value to any government employees of other countries.

The Company does not tolerate or endorse corruption in the marketplace. Employees must ensure that payments made by or on behalf of the Company are made only for legitimate business purposes. Under no circumstances is it acceptable to offer, give, solicit or receive any form of bribe or kickback. The Company is committed to complying with the Foreign Corrupt Practices Act, the OECD Convention on Combating Bribery of Public Officials in International Business Transactions and the UK Bribery Act of 2010, and any other anti-bribery and corruption statute in each foreign country in which the Company does business. Due to the complex laws in this area, you should also refer to the Company's Foreign Corrupt Practices Act Policy and Company Anti-Bribery and Corruption Policy and consult with the Compliance Officer and General Counsel of the Company with any questions and/or concerns.

Money Laundering or Illicit Financing

Employees must actively guard against the use of the Company's products and services by third parties for the purposes of money laundering or illicit financing activity, including terrorist activity. Money laundering is the process by which the proceeds of criminal activity are moved through the financial system in order to hide all traces of their criminal origin. Money laundering is an essential part of much criminal activity and has become the focus of considerable attention by governments, international organizations and law enforcement agencies throughout the world. By contrast, illicit financing activity, including activity by or for terrorist groups, focuses on the destination and use of funds that may come from legitimate or criminal sources, or a combination of the two.

The Company is committed to cooperating fully with law enforcement and regulatory investigations concerning possible money laundering or illicit financing activity. You must immediately contact the Company's General Counsel and Compliance Officer if you are approached in any manner by government agencies for records and information on customers, agents, or business partners that may be under investigation. Strict rules specify time frames for complying with such government inquiries or requests and for reporting certain activities that may bear upon money laundering or terrorist activity. Therefore, your immediate action is vital in both reporting requests and being responsive when given instructions by the General Counsel and Compliance Officer.

Corporate Criminal Offences ("CCOs") of Failure to Prevent the Facilitation of Tax Evasion Company policy:

The Company is committed to complying with its obligations under the UK Criminal Finances Act 2017 ("CFA 2017") which introduced a new corporate criminal offences relating to the Failure to Prevent the Facilitation of Tax Evasion.

Background and further guidance:

It is already a crime to deliberately and dishonestly facilitate tax evasion by another person, or to be knowingly involved in the fraudulent evasion of tax by another. The CFA 2017 introduced two new corporate criminal offences of the Failure to Prevent the Facilitation of Tax Evasion. Penalties under the CCOs are severe, including unlimited fines and ancillary orders (such as confiscation orders), along with significant reputational damage The CCOs comprise two offences: (i) the facilitation of UK tax evasion; and (ii) the facilitation of non-UK tax evasion. The Company may be in breach of the CCOs if it fails to prevent the facilitation of tax evasion by an "associated person" (see definition below), acting for or on behalf of the company.

A CCO breach may occur when:
1. Taxes have been evaded (by either an individual or a legal entity);
2. An "associated person" has criminally enabled or facilitated the tax evasion.; and
3. The company has insufficient reasonable prevention procedures to prevent its associated person from facilitating tax evasion.
This means that the Company will be criminally liable unless it can successfully raise the defence that it had reasonable prevention procedures in place.

"Tax evasion" is conduct that constitutes the common law offence of cheating the public revenue, or the statutory offences of fraudulently evading taxes. Tax evasion is not the same as tax avoidance or tax planning. Tax avoidance is not illegal, and involves taking steps, within the law, to minimize tax payable (or maximize tax relief). However, tax evasion involves deliberately and dishonestly using illegal practices to not pay taxes due. An example of tax evasion is when a person knows that they have a tax liability and follows through on a dishonest intention not to declare it.

"Associated person(s)" are any persons (whether individuals or corporate entities) performing services for or on behalf of Company. This includes employees, agents, contractors, third party services providers, suppliers and subsidiary companies, when they are acting in the capacity of an associated person of Virtusa at the material time.

The Company's approach to its obligations under the CFA 2017:

The Company takes a zero-tolerance approach to tax evasion and requires its employees and associated persons to adhere to this policy. The Company, its employees and other associated persons shall not knowingly take any part, or participate, in any tax evasion conduct and must take all reasonable steps to prevent tax evasion by third parties acting on its behalf (e.g. subcontractors) and/or being knowingly concerned in the facilitation of tax evasion. This includes not participating in transactions where tax evasion by a third party is suspected. Where tax evasion is suspected, employees and contractors must promptly report to the General Counsel and Compliance Officer, at the earliest available opportunity who may then deal with their suspicions in accordance with local suspicious activity reporting requirements.

Practical example of a CCO breach:

Situation*:* As part of Company negotiations with a new supplier, that supplier suggests that it would be possible to get a lower price if the Company were to make their payment without the supplier having to issue an invoice.

Response: It is not acceptable to pay suppliers unless the Company is in receipt of a valid invoice. The lower price being offered for payment without an invoice is potentially because the supplier is not intending to include the payment in their reported revenue, thereby evading the payment of tax on that income. Any employee agreeing to such an arrangement could be facilitating the evasion of tax by the supplier and the Company could therefore be liable to criminal prosecution under the CFA 2017.

Labor and Employment

The Company adheres, and expects its employees to adhere, to all federal, state, and local laws regarding labor and employment. These include but are not limited to equal employment opportunity, harassment and discrimination, and safety and health.

Quality of Public Disclosures

The Company is committed to providing its stockholders with complete and accurate information about its financial condition and results of operations as required by the securities laws of the United States. It is the Company's policy that the reports and documents it files with or submits to the Securities and Exchange Commission, and its earnings releases and similar public communications made by the Company, include fair, timely and understandable disclosure. Officers and employees who are responsible for these filings and disclosures, including the Company's principal executive, financial and accounting officers, must use reasonable judgment and perform their responsibilities honestly, ethically and objectively in order to ensure that this disclosure policy is fulfilled. The Company's Disclosure Committee and senior management are primarily responsible for monitoring the Company's public disclosure.

Compliance Procedures

All directors, officers and employees will be supplied with a copy of the Code upon its adoption by the Company. In addition, all directors, officers and employees will be supplied and asked to confirm in writing that they have read and understood, and will comply with, the Code at the beginning of their service at the Company. Updates of the Code will be provided from time to time. A copy of the Code is also available to all directors, officers and employees by requesting one from the Compliance Officer or Human Resources department, or by accessing the Company's website at www.virtusa.com.

Monitoring Compliance and Disciplinary Action

The Company's management, under the supervision of its Board of Directors or a committee thereof or, in the case of accounting, internal accounting controls or auditing matters, the Audit Committee, shall take reasonable steps from time to time to make a preliminary assessment of where the matter should be allocated and addressed and (i) to monitor and test compliance with the Code with respect to matters under its supervision as set forth above, and (ii) when appropriate, impose and enforce appropriate disciplinary measures for violations of the Code, after making a preliminary assessment of where the matter should be properly allocated and addressed.

Disciplinary measures for violations of the Code may include, but are not limited to, counseling, oral or written reprimands, warnings, probation or suspension with or without pay, demotions, reductions in salary, termination of employment or service and restitution.

The Company's management shall periodically report to the Board of Directors or the Corporate Governance Committee on these compliance efforts including, without limitation, periodic reporting of alleged violations of the Code and the actions taken with respect to any such violation.

From time to time (no less than annually), the Company will also train all relevant employees (i.e., those who interact with the government or perform, finance, procurement, HR or business functions) and have global communications on a regular basis to ensure the employees are aware of the critical sections of the Code, including the FCPA, and UK Bribery Act compliance and how they may report suspected corruption and bribery.

The Company will also provide training to any other employees or directors the Company deems appropriate.

The Company shall conduct periodic audits of the Company's compliance programs and compliance with the Code, including FCPA, UK Bribery Act and anti-corruption compliance programs and processes of the Company.

Reporting Concerns/Receiving Advice

Communication Channels

Be Proactive. A copy of the Code will be maintained on the Company's website at www.virtusa.com. Every employee is encouraged to act proactively by asking questions, seeking guidance and reporting suspected violations of the Code and other policies and procedures of the Company, as well as any violation or suspected violation of applicable law, rule or regulation arising in the conduct of the Company's business or occurring on the Company's property. **If any employee believes that actions have taken place, may be taking place, or may be about to take place that violate or would violate the Code, he or she is obligated to bring the matter to the attention of the Compliance Officer.**

Seeking Guidance. The best starting point for an officer or employee seeking advice on ethics-related issues or reporting potential violations of the Code will usually be his or her supervisor. However, if the conduct in question involves his or her supervisor, if the employee has reported the conduct in question to his or her supervisor and does not believe that he or she has dealt with it properly, or if the officer or employee does not feel that he or she can discuss the matter with his or her supervisor, the employee may raise the matter with the Compliance Officer.

Communication Alternatives. Any officer or employee may communicate with the Compliance Officer by any of the following methods:

- In writing (which may be done anonymously as set forth below under "Reporting; Anonymity; Retaliation"), addressed to the Compliance Officer, by U.S. mail to c/o Virtusa Corporation, 132 Turnpike Road, Suite 300, Southborough, MA 01772;
- **By e-mail using a web based submission tool** http://www.openboard.info/VRTU/ **(which may be done anonymously as set forth below under "Reporting; Anonymity; Retaliation"); or**

By phoning an off-site voicemail account named Whistleblower Hotline which we have established for receipt of questions and reports of potential violations of the Code. The off-site voicemail account may be reached at (US/Domestic) 1-844-403-4964 & (International) 402-999-0449 and calls may be made anonymously as set forth below under "Reporting; Anonymity; Retaliation".

Additional Resources for Questions and Reporting

- **General Counsel and Compliance Officer**
- By Email: ptutun@virtusa.com • By Phone: 508-389-7450

You may call or report via the web anonymously or you can give your name. If you give your name, your identity and the information you provide will be shared only on a "need to know" basis with those who are involved in addressing your concern.

Reporting Accounting and Similar Concerns. Any concerns or questions regarding any Company policy or procedure or applicable law, rules or regulations that involve accounting, internal accounting controls or auditing matters should be directed to the Audit Committee or a designee of the Audit Committee. Officers, employees or any other party may communicate with the Audit Committee or its designee:

- in writing to: Chairman of the Audit Committee, c/o Virtusa Corporation, 132 Turnpike Road, Suite 300, Southborough, MA 01772; or
- **by phoning the Whistleblower Hotline (US/Domestic) 1-844-403-4964 & (International) 402-999-0449**

Officers and employees may use the above methods to communicate anonymously with the Audit Committee.

You may also report any such violations or ask questions by using the following:

- ***General Counsel and Compliance Officer***
- By Email: ptutun@virtusa.com
- By Phone: 508-389-7450

Misuse of Reporting Channels. Employees must not use these reporting channels in bad faith or in a false or frivolous manner. Furthermore, employees should not use the off-site voicemail account to report grievances that do not involve the Code or other ethics-related issues.

Director Communications. In addition to the foregoing methods, a director may also communicate concerns or seek advice with respect to this Code by contacting the Board of Directors through its Lead Director, or a committee thereof responsible for administering and interpreting this Code.

Reporting; Anonymity; Retaliation

When reporting suspected violations of the Code, the Company prefers that officers and employees identify themselves to facilitate the Company's ability to take appropriate steps to address the report, including conducting any appropriate investigation. However, the Company also recognizes that some people may feel more comfortable reporting a suspected violation anonymously.

If an officer or employee wishes to remain anonymous, he or she may do so, and the Company will use reasonable efforts to protect the confidentiality of the reporting person subject to applicable law, rule or regulation or to any applicable legal proceedings. In the event the report is made anonymously, however, the Company may not have sufficient information to look into or otherwise investigate or evaluate the allegations. Accordingly, persons who make reports anonymously should provide as much detail as is reasonably necessary to permit the Company to evaluate the matter(s) set forth in the anonymous report and, if appropriate, commence and conduct an appropriate investigation.

No Retaliation

The Company expressly forbids any retaliation against any officer or employee who, acting in good faith, reports suspected misconduct. Any person who participates in any such retaliation is subject to disciplinary action, including termination.

Waivers and Amendments

No waiver of any provisions of the Code for the benefit of a director or an executive officer (which includes without limitation, for purposes of this Code, the Company's principal executive, financial and accounting officers) shall be effective unless (i) approved by the Board of Directors or, if permitted, the Audit Committee (or the committee of the Board to whom the matter has been allocated or referred) , and (ii) if applicable, such waiver is promptly disclosed to the Company's stockholders in accordance with applicable U.S. securities laws and/or the rules and regulations of the exchange or system on which the Company's shares are traded or quoted, as the case may be.

Any waivers of the Code for other employees may be made by the Compliance Officer, the Board of Directors or, if permitted, a committee thereof.

All amendments to the Code must be approved by the Board of Directors or a committee thereof and, if applicable, must be promptly disclosed to the Company's stockholders in accordance with applicable U.S. securities laws and/or the rules and regulations of the exchange or system on which the Company's shares are traded or quoted, as the case may be.

Information Security Declaration Form

*With respect to Virtusa Corporation, including affiliates and subsidiaries ("**Virtusa**") providing access to its information assets or to that of its clients or group companies, for carrying out my obligations, I, the undersigned, hereby make the following declaration:*

1. *I confirm that I have read and fully understood "Information Security – User Handbook" and the policies and procedures of Virtusa concerning information security and shall confirm to the same during the period of my employment with Virtusa.*

2. *I undertake to read and understand the information security training material(s) and complete the ISMS Certification exam within one month of my joining Virtusa.* ***Failure to comply with this certification policy may lead to disciplinary action taken against me, including stoppage of salary.***

3. *I agree to review and abide by the information security policies of the client(s) of Virtusa while providing services to the client(s) of Virtusa.*

4. *I agree that Virtusa may take any disciplinary action as per HR Manual and Guidelines on HR Actions for Information Security Violations against me in the event of me violating any of the information security policies and procedures of Virtusa or its group companies or that of its client(s).*

EXPORT LICENSING COMPLIANCE - LETTER OF ASSURANCE FOR EMPLOYEES

***Attn**: Export Licensing Coordinator*
***Re**: No Re-export of Controlled Technical Data or Software*

During my employment with Virtusa (individually and together with its parent, subsidiaries and/or affiliates, "Virtusa Group"), I have or will have access to proprietary technical data and computer Software. As a foreign national (for U.S. operations; defined as a non-U.S. citizen without U.S. permanent residency status, offshore; nonresident of local business country location), I understand that this access constitutes an export of technical data/ Software from the United States and is therefore governed by the provisions of the U.S. Export Administration Regulations ("EAR").

Consequently, I hereby agree to comply with U.S. Export Administration Regulations as they pertain to any technical data or computer software to which I have access during my Virtusa Group employment. Unless prior written authorization is received from the U.S. Department of Commerce or other appropriate agencies, I shall not knowingly re-export, directly or indirectly, this technical data/computer software without full compliance with U.S. export control laws. In particular, I will not export it to any of the following nations or nationals of:

1. Country Group E Cuba, Iran, Libya, North Korea, Sudan, Syria, or
2. Non-civil (i.e., military) end-users or for any non-civil (i.e., military) end uses in Country Groups D: 1

(currently Albania, Armenia, Azerbaijan, Belarus, Bulgaria, China (PRC), Cambodia, Estonia, Georgia, Iraq, Kazakhstan, North Korea, Kyrgyzstan, Laos, Latvia, Lithuania, Macau, Moldova, Mongolia, Romania, Russia, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, and Vietnam.

I will comply with any future modifications of the foregoing list of restricted destinations by amendments to the U.S. Export Administration Regulations or other U.S. Government agencies, which will be posted at http://www.access.gpo.gov/bis/ear/ear_data.html.

Without the prior approval of the U.S. Department of Commerce or other appropriate agencies (which shall be sought by Virtusa Group if and where appropriate), I shall not knowingly export to any of the above nations, directly or indirectly, any product (or any part thereof), process or service which is the direct product of this technical data/computer software .

Additionally I understand that countries other than the U.S. may restrict the import or use of strong encryption products and export of any products, and I will comply with any such restrictions. In the event that I have questions about any such restrictions, I will contact a Virtusa Group Export License Coordinator.

I understand that my failure to comply with the requirements and restrictions set forth in this letter may expose me and Virtusa Group to severe criminal and administrative penalties and sanctions. In addition, I will be subject to disciplinary action up to and including immediate termination of my Virtusa Group employment.

By signing below I agree to comply with the requirements and restrictions set forth in this letter, which agreement I understand is a condition to my having access to proprietary technical data and/or computer software during my Virtusa Group employment.

Data Privacy Consent Form

I understand Virtusa Corporation,including affiliates and subsidiaries ("Virtusa"), collects, receives, possesses stores, deals or handles personal information including sensitive personal data or information to provide the required services to its Employees for business and legal / regulatory purposes.

In order to provide essential services to Employees, Virtusa shall collect information as required, including but not limited to, the following:

- *ID Proof (PAN card, Passport, Driving license, Voters' ID or any valid Government ID proof)*
- *Address Proof (Passport, Driving license, Voters' ID, Bank Statement, Ration Card etc)*
- *hotline Contact Information (Address, Phone number, Email ID, Emergency contact personnel information etc.)*
  - *Demographic information (Age, Gender, Educational qualification, Personal interests etc.)*
- *Bank Account Details*

Virtusa shall collect information through different means, including but not limited to:

- *Joining kit*
- *Various applications like Empower, Adrenalin, PeopleSoft, Octopus etc*

I understand that the information provided shall be processed/accessed by various stakeholders like internal functions (HR, Finance, Delivery team) and external stakeholders (like Clients / BGC Vendors) for lawful business purposes.

I understand that the personal information collected from Employees shall be shared with third parties under lawful contract or with any Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity; prevention, detection, and investigation of incidents (including cyber incidents) and prosecution and punishment of offences.

I understand Virtusa has established and implemented reasonable security practices and procedures to ensure security of the personal information of Employees collected. The Enterprise Data Privacy Policy (Virtusa Policy portal ->; Human resources ->; Talent compliance ->; Enterprise Data Privacy Policy) and Virtusa Global Workforce Privacy Notice (Virtusa Policy portal ->; Human resources ->; Talent management ->; Virtusa Global Workforce Privacy Notice) of Virtusa Provides details on collection, usage and disposal of personal information.

I understand that as a provider of the personal information, that I have the option to refuse providing data or information sought by Virtusa. If I do not provide the required personal information, Virtusa shall opt not to provide the essential services for which the said information was sought

I hereby give my consent to Virtusa to collect, possess, store, handle and process my "Personal information (Including Sensitive Personal data or information) for the purpose of providing business services including sharing with business partners as applicable.

I hereby represent that the Personal Information shared by me is correct and accurate. Further, I hereby agree to indemnify Virtusa against all claims raised against Virtusa by including but not limited to third parties, Governmental Agency, on the accuracy/correctness of the Personal Information provided by me

"Personal Information" is any information that relates to a natural person, which either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.

"Sensitive personal data or information" means such personal information which consists of information relating to:

1. *Password*

2. *Financial information such as Bank account or credit card or debit card or other payment instrument details*

3. *Physical, physiological and mental health condition*

4. *Sexual orientation*

5. *Medical records and history*

6. *Biometric information*

7. *Any detail relating to the above clauses as provided to body corporate for providing service, and*

8. *Any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.*

9. *Personal information shall not include information that is lawfully obtained from publicly available information or from Central/State or local Government records that are made available to the general public.*

Software Compliance - DO's and DON'Ts

Virtusa Corporation, including its affiliates and subsidiaries ("Virtusa"), respects the Intellectual Property of all software publishers and insists that all users working for Virtusa, also follow the terms of use as per the license agreements of each software publisher. It is important that each user is aware of the Virtusa software Licensing Compliance Policy and software Usage Policy. The gist of these policies is mentioned in the following Do's and Don'ts. It is a must that all users working for Virtusa abide by the software terms of use and other intellectual properly laws to maintain 100% compliance at all times . Please acknowledge your acceptance to abide, by reading and signing the below compliance sheet.

Commercial Software Licenses

- *Commercial software can only be used with a license*
- *Every commercial software will have "Terms of use" mentioned in its license agreement. Please ensure that software is strictly used as per these terms*
- *Commercial software should NOT be installed without clearance from Compliance Team*
- *Dumps/Repositories of commercial software are NOT allowed. Do NOT keep software setup files of the client on your systems.*
- *Do NOT distribute setup files without clearance from Software Compliance Team. Please hand over commercial software setup files to IT Team formally.*
- *Software license keys should NOT be shared*
- *If software needs a client or browser for connectivity, all linkages to servers can be tracked by auditors. Please have a license copy specifically for the authorized server and do NOT connect to any other server.*

Customer Software

- *Customer software can ONLY be used after written authorization from the customer containing license copy, tripartite agreement, email mentioning the user(s) machine(s) on which it is to be installed, period of usage and geography of usage. This should be approved by Compliance Team*
- *Software belonging to one project should NOT be used for another project.*
- *Client license keys can ONLY be used for the client's project. On NO account should the customer's key be used for any other project*

Evaluation Software

- *Evaluation software should NEVER be used on production machines. Please abide by terms of use of the End User License Agreement (EULA).*
- *Evaluation software should NEVER be used to connect to Customer machines. Auditors will treat this as production use*

Unapproved Categories of Software

- *Cracks, Torrents, CD/DVD Burners, commercial software without license, are strictly prohibited*

Version/Edition License Compliance

- *Software is licensed for a particular version/edition. Do NOT use a later version/edition than what is authorized*

- *Be aware of the Licensing type before usage (per seat/concurrent/named user/processor based/etc) & follow the type of usage permitted*

Uninstallations

- *Uninstalling commercial Software does not necessarily reduce liability. So ensure license is available, BEFORE the installation is done. Uninstallation of commercial software should be performed by the IT team. Please raise helpdesk tickets to communicate uninstallation requirements.*

Downloads/Uploads

- *Do NOT download or upload illegal software over the internet. Identified Instances of software piracy and software misuse will have serious repercussions.*

Message from the Enterprise Risk Management Organization

Please be informed that absolutely any references to or about Virtusa Corporation, including its affiliates and subsidiaries ("Virtusa"), its customers, projects, processes, methodologies etc. must not be published by any employee on any Web site or communicated verbally to any unauthorized person, either within or outside of Virtusa, without prior approval by the Enterprise Risk Management Organization. This is considered to be a serious breach of our organizational information security policy and the Non-Disclosure Agreement that all employees and contractors sign before coming on board. Given the severity of this violation, it might even attract 'immediate termination' as disciplinary action.

In addition, ***including details about Virtusa's customers, projects worked on, etc. in resumes hosted on job / career portals is also strictly prohibited*** *and is in violation of our security policy and employee NDA.*

All employees also carry the responsibility of bringing security incidents to the notice of the Enterprise Risk Management Organization.

Consent Note

I hereby confirm to have read the following documents/forms and agree to comply with the following and all other Company's policies in this regard:

1. ***Code of Conduct***
2. ***Message from the Enterprise Risk Management Organization***
3. ***Software Compliance - DO's and DON'Ts***
4. ***Information Security Declaration Form***
5. ***Data Privacy Consent Form***
6. ***Export Licensing Compliance - Letter of Assurance***

Employee Signature :

Name:N Harish Kumar

Date of Signing:

Remote Work Agreement Acknowledgement Form

When I am given remote working capabilities, I understand that I occupy a position of trust and have been provided the remote working capability, by my role with Virtusa/Client, to operate remotely and provide services to Virtusa/Client.

As a recipient of Virtusa and Client information and information assets (including soft tokens), I agree to comply with the following:

1. Proprietary Information: Although I am provided with the remote working capability, I am aware that all information / information assets of Virtusa and Client, in any form, are their sole property.

2. Business purposes: I am aware that I have been provided access to the Information assets of Virtusa & Client for business purposes only. I will be working only from home and not from any other kiosks or any unsecured location or internet cafe.

3. Acceptable usage: I shall comply with the Information Security policies and guidelines of Virtusa and Client and handle assets / data accordingly.

a. Entitlements: I shall

i. Access / use only as per the entitlements provided
ii. Not access or disclose any source code, data, information or documention to any individual or organization unless specifically authorized to do so, by the information owner
iii. Refrain from gaining privileges that are over and above my roles and responsibilities
iv. Refrain from circumventing any security measure, control or system which has been implemented to restrict access to secure area, computers, networks, systems or information
v. Refrain from misusing the system and the remote working capability provided
vi. Refrain from using or inserting any USB or hard disks & connecting any personal printers to the Virtusa/Client system

b.Reasonable Safeguards: I shall

i. Ensure that the laptop or virtual workplace are not shared with family members, Virtusa's or Client' competitors or their employees, at any time and for any purpose
ii. Ensure that reasonable safeguards are in place to prevent shoulder surfing, or unauthorized access to information
iii. Ensure that the Anti-Virus and Anti Spyware is up to date
iv. Promptly report any unauthorized use or loss of any identification codes, passwords or Information assets to the right authority
v. Use only the provided laptop or remote work capability to connect to Virtusa/Client environment
vi. Use only software that is authorized by Virtusa on the laptop and workspace
vii. Refrain from downloading or using unauthorized software and application without the appropriate approval viii. Refrain from introducing any contaminant into any system, or computer network or Client environment through the Virtusa or client provided laptop
viii. Not download, install or run security programs or utilities that reveal or exploit weaknesses in the Virtusa or Client systems and networks

ix. Refrain from utilizing the laptop or the remote work capability for personal benefit, unsolicited advertising, unauthorized fund raising, promoting political or religious agenda, or participating in any controversial or illegal activity (like supporting terrorist agenda or viewing / downloading pornographic material)
x. Refrain from storing personal files and documents (like email messages, voice messages, photos, music files and personal files)
xi. Refrain from downloading Virtusa/Client information in local environment or share such information via email to Virtusa or personal email IDs
xii. Refrain from forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender
xiii. Refrain from leaving the laptop unattended even for a minute
xiv. Refrain from connecting the assets to public hotspots & Wi-Fi due to data risk
xv. Report any breach of the Client policy or guideline immediately to the right authority
xvi. Do not use any recording equipment like CCTV, Mobile Camera, Digital camera, or any other mechanisms to record or capture the screen when working on Virtusa/Client environment

4. I understand that I shall be subjected to monitoring when using Virtusa/remote work, and Client information and Information assets.

5. If I am found to violate Virtusa or Client policies and guidelines, I shall be subjected to disciplinary action, deemed appropriate by Virtusa and Client, up to and including termination of employment.

Signature:
Employee number/code: 8176687
Name: N Harish Kumar **Date of signing:**

SELF DECLARATION REGARDING MY MEDICAL FITNESS

I N Harish Kumar, 8176687 an employee of Virtusa Consulting Services Private Ltd, hereby make the following declaration regarding my medical fitness, namely:

1. **Medical Fitness Declaration:**
   I declare that, to the best of my knowledge, I am in good physical and mental health and capable of performing the duties and responsibilities expected of me in the role I will be assigned by the Virtusa Consulting Services Private Ltd.

2. **Workplace Health & Safety:**
   I will promptly inform the company's human resources or management team should any medical condition arise, that may affect my ability to perform my duties or pose a risk to my health and safety and that of the others at the workplace. I also authorize the company to contact my emergency contact person in the event of such a situation.

3. **Liability and Compliance:**
   I understand that it is my responsibility to ensure that I am fit to perform the required tasks assigned to me and that failure to disclose any medical conditions or non-compliance with health and safety protocols could result in consequences, including but not limited to disciplinary action, reassignment of job duties.

   By signing below, I confirm that I have read, understood, and agreed to the terms of this declaration.

Employee Signature:

Employee Name: N Harish Kumar

Employee ID: 8176687

Date:

This document ensures that the company is aware of the medical fitness status of the employee and allows for proper action to be taken if any medical conditions affect their ability to perform job-related tasks.

Declaration of PAN & Aadhar Card

I, N Harish Kumar, hereby confirm that the linkage between Aadhar & PAN card (details of which are given below) is completed from my end.

Aadhar No: 766189037459
Name as per Aadhar Card: N Harish Kumar
PAN No: CSQPN6897Q
Name as per PAN card: N Harish Kumar
Mobile Number linked to Aadhar Card: +91-9440125007

If not completed, I hereby undertake the responsibility to complete the activity immediately and provide the necessary details on or before 13-Aug-25.

Regards

Candidate Name: N Harish Kumar
Emp ID / Candidate ID: 8176687
Date: 05 August 2025
Signature:
Date of Signing: