virtusa

EMPLOYEE DECLARATION ACCEPTABLE USE OF ASSETS

I Totakura Madhu Shantan,
declare that I have read, understood and shall abide by the Acceptable Use of Assets terms ("Asset Security Terms") during my employment with Virtusa Consulting Services Private Limited ("Virtusa").

I have read and understood the company policies, security requirements and will abide by the expected behavior from the employees and their obligations related to the use of information assets provided by Virtusa and /or Virtusa's Clients or the assets used for Virtusa business purposes irrespective of the place of work (Virtusa premise, Client premise, WFH or any other location).

I understand that I occupy a position of trust and have been provided access, by virtue of my role with the Virtusa/ Virtusa's Client. As an employee of Virtusa, I agree to abide by the following terms regarding security:

Desktops, Laptops & Servers

- I will never disclose identification codes (User ID, Access card, Log-in-ID), Virtusa or Client system credentials (login ID, passwords) with anyone
- I will not write down my passwords or store it in an insecure manner
- I will not use automatic logon functionality in browsers or applications
- I will not ask or use a password of another person
- I will adhere to "Clear screen and Clear desk" policy
- I will ensure that active sessions with Client or any confidential documents are closed before providing remote access rights to IT team or any other team
- I will ensure Virtusa/Client assets are protected from misuse/mishandling/unauthorized access at all times
- I will store Virtusa or Client information only in authorized and approved locations
- I will ensure that endpoints are compliant with security requirements
- I will not move any Virtusa or Client assets without prior written authorization from Virtusa or the Client
- I will not use any unauthorized devices to access Client/Virtusa systems
- I will not use or install unauthorized software on Virtusa or Client systems
- I will not use unauthorized communication channels for business purposes
- I will never use any non-Virtusa or non-Client assets to access Virtusa/Client owned/controlled information systems, without prior written authorization. Such devices will be deemed as unauthorized devices, unless explicitly authorized

Network and System Assets

- I will not perform port scanning or network security scanning unless such actions are pre-approved in writing by the e Security Team

- I will not intercept data by monitoring the network unless it is part of my roles & responsibilities and unless such actions are pre-approved in writing by the Security Team

- I will not create honeypot or similar technology on the Virtusa/Client network unless it is my regular job that has been assigned in writing by the concerned team

- I will not use any devices or tools to circumvent any security controls established or to introduce vulnerabilities in to the Virtusa/ Client network or systems

- I will ensure that my Virtusa/Client assets are regularly updated with the latest virus and patch updates

- I will ensure that privileged access obtained via exception approvals is strictly used for the purpose it was pre- approvedfor and up to the time frame it is approvedfor

- I will not use administrator privileges to create or reset the local Administrator account password

- I will not introduce any malicious programs into the network or systems (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.)

- I will not install or distribute any software without the guidelines from the IT team and a valid service request

- I will not uninstall approved Virtusa/Client software available in the asset

- I will not uninstall/disable/modify any installed security tools

- I will not create/modify/remove any user accounts

- I will not create shared folders with read/write access to all domain users

- I will not modify the system time

Internet

- I will use Virtusa/Client provided Internet services for business purposes only.

- I will not upload Virtusa or Client information in any unauthorized sites (E.g. Dropbox, Google drive, GitHub, online file conversion sites, compilation sites) or with any third parties, unless it's pre-approved and is required as part of my allocated job

- I will not bypass filtering or monitoring, or other access controls set forth by the IT services department to gain or enhance access to internet

- I will not establish connections that could allow non-Virtusa/non-Client employees to gain access into Virtusa/Client systems and information assets

• I will not view/produce/store indecent, offensive, illegal, or sexually explicit material in Virtusa/Client systems and information assets

• I will not use Virtusa/Client logos or information to express personal views or identity in any web page or social media unless it has been approved in writing, in advance, by the Virtusa/Client management

• I will not share any information about the company or the process of the company or about an executive or officers or style of their practices or the work culture in social media or in personal/public web page or blogs or other forum/medium either directly or indirectly

• I will not reveal or publicize proprietary or confidential information unless authorized to do so

• I will not make fraudulent offers of Virtusa/Clientproducts, items, or services

• I will not use copyrighted information/ software downloaded from the internet

• I will not use/exploit Virtusa/Client assets and logos for religious, racial, ethnic or terrorism related activities

• I will not release any Intellectual property owned by the organization unless authorized in writing prior to such release by the relevant Virtusa team

• I will use cloud infrastructure in a responsible manner and ensure the privileges are used for the authorized business requirement

• I will not make any change which could degrade cloud infrastructure security without proper prior written approvals

• I will not store any sensitive information in cloud environments without appropriate prior written approval

Email and Communication Assets

• I will use email and communication assets provided by Virtusa/Client for business purposes only

• I will not download or open attachments or links from unknown or unauthorized sources

• I will not send any unsolicited, junk mail or spam, pornographic, defamatory, obscene, or harassing emails that would harm individuals within and outside of Virtusa

• I will not share Virtusa/Client confidential information to any non-Virtusa/Client email id without obtaining prior written approval from the appropriate management representative and without subjecting such disclosure to the same extent of written confidentiality obligations as I am bound to under my employment agreement with Virtusa.

• I will not send Virtusa or Client related information/mails to personal email accounts

• I will not share Client related information to any non-Client email id, unless it is for an authorized business purpose

• I will not share Virtusa/Client related information to anyone who is not authorized to view the information

• I will not auto forward or send information from Client email address to Virtusa email address unless it is for an authorized business purpose

• I will not send any confidential information from Virtusa email address to Client email address unless it is for an authorized business purpose

• I will not enable automatic forwarding of e-mail to Client domain/Virtusa domain addresses

• I will not send any work-related emails using a personal email

• I will not use Virtusa or Client collaboration platforms to promote political agendas, communicate irrelevant or obscene messages, share information in an unauthorized manner or misrepresent facts

• I will not use Virtusa/Client e-mail address for any subscriptions on sites or mailing lists, to post in any forum or social media

• I will not use Virtusa/Client e-mail to generate spam

• I am aware that all activities within Virtusa/Client information systems will be monitored with or without notice for the following reasons. However, personal information will be excluded as per the local laws of the land and relevant regulatory requirements

- To monitor performance
- Ensure compliance with Virtusa/Client policies
- Prevent misuse of the Systems
- Troubleshoot hardware and software problems
- Comply with legal and regulatory requests for information, and
- Investigate disclosure of confidential business, proprietary information, or conduct that may be illegal or adversely affect Virtusa or its employees
- To support incident investigation

• Prior to sending any email, I will ensure that classification of the email is done as per Virtusa/Client data classification standard

Telephone, Printers and Scanners

- I will use telephone, printers, and scanners for business purposes only

- I will refrain from leaving messages containing sensitive Virtusa/Client information on answering machines or voice-mail systems

- I will not record discussions unless authorized by all participating entities

- I will not use the camera in mobile phones or any other camera inside Virtusa/Client premises or take photo of the screen (either my system of any other Virtusa/Client systems)

VPN Tokens

- I will be responsible for Customer or Virtusa two factor authentication tokens and its use

- I will not disclose VPN token numbers/ details used for connecting to Virtusa/Client network

- I will promptly report token misplacement to the Virtusa/Clienti ncident reporting team

BYOD

- Prior to enrolling into BYOD program, I understand that I should abide by the applicable policies, including acceptable use and data protection of Virtusa and Client data

- I will ensure that the privileges are used for the intended and declared purpose and will take necessary precautions to ensure confidential data is kept secure

- I am aware that rooted (Android) or jail broken (iOS) devices are strictly forbidden from accessing the Virtusa/Client network
- I will not store Virtusa or Client data on personal devices under any circumstances

- I shall ensure that devices used for BYOD Virtusa apps are owned by me and will be in my possession always

- I am aware that upon termination of the services or upon termination of my employment with Virtusa, all corporate data on the mobile device will be wiped/deleted for security purposes. I will not store or forward, Virtusa/Client data on other personal devices than approved devices, cloud services or any other storage mechanism

- I am aware and shall ensure that my personal device will be remotely wiped if device is lost

- I am aware and shall ensure thatto prevent unauthorized access, devices must be password protected with a strong password

- I am aware standard policies will be applied to protect corporate data

- I am aware device will be retired if IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure

- I will not store, forward or move, company data to other unauthorized devices

- I am aware and shall ensure that any personal cellphone/camera phone usage while on site should be as per the Virtusa/Client security guidelines

General Use and Ownership

• I am aware that all information / information assets of Virtusa and Client, in any form, are their sole property

• I am aware that access from home would only be as per the entitlements provided and as per the work from home rules/policies of Virtusa.

• I am aware Virtusa policies shall be applicable even when travelling or operating from remote locations and I should abide by the Asset Security terms when using company assets or accessing company information resources

• I will notbring any mass storage devices (e.g., CD, Hard Disc, USB etc.,) inside Virtusa/Client premises unless it is for an authorized business purpose

• I will use any additional privileges granted (e.g., USB, admin rights etc.) for designated business purpose only

• I will not share physical ID / access badges, which are provided for my use with anyone

• I will ensure appropriate management written approval is sought for the use of removable media within Virtusa

• I will not use Intellectual Property, including copyrighted material, trademarks and trade-secrets of other organizations or entities without appropriate management approval

• I will fully cooperate with audit / reviews conducted by IT department or Security team of Virtusa/Client

While Working from Home

• I will not access or disclose any source code, data, information, or documentation to any individual or organization unless specifically authorized to do so in writing, by the information owner

• I will refrain from gaining privileges that are over and above my roles and responsibilities

• I will refrain from using the system and the remote working capability provided in contravention of the applicable rules and policies of Virtusa/Client

• I will refrain from using or inserting any USB or hard disks & connecting any personal printers to the Virtusa/Client system

• I will ensure that Virtusa/Client 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

• I will ensure that reasonable safeguards are in place to prevent shoulder surfing, or unauthorized access to informationon Virtusa/Client laptops

• I will promptly report any unauthorized use or loss of any identification codes, passwords, or Information assets to the right authority

• I will only use the provided laptop or remote work capability to connect to Virtusa/Client environment

• I will refrain from introducing any contaminant into any system, or computer network or Client environment through the Virtusa or Client provided laptop

• I will not download, install, or run security programs or utilities that reveal or exploit weaknesses in the Virtusa or Client systems and networks on Virtusa laptops

• I will 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)

• I will refrain from storing personal files and documents (like email messages, voice messages, photos, music files and personal files)on Virtusa/Clientlaptops

• I will refrain from downloading Virtusa/Client information in local environment or share such information via email to Virtusa or personal email ID

• I will refrain from forging, misrepresenting, obscuring, suppressing, or replacing a user identity on any electronic communication to mislead the recipient about the sender

• I will refrain from leaving the Virtusa/Clientlaptop unattended even for a minute

• I will refrain from connecting the assets to public hotspots, Wi-Fi like airports, cafes etc. and ensure to report any breach of the Client policy or guideline immediately to the right authority

• I will 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

Policy Compliance

I understand compliance with the Acceptable Usage policy is mandatory and any exception should be approved by the respective stakeholder.

Consequences of Violation of this Policy

I understand that violation of any Virtusa or its Client's policies will be considered as a security incident and disciplinary action taken will be consistent with the severity of the security incident as determined by an investigation conducted by Virtusa/Client. This may include, but will not be limited to:

• Loss of access privileges to information assets,

• Removal of any exceptions provided,

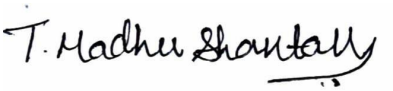
• Disciplinary actions in-line with the Virtusa/Client disciplinary policy, and

• Other actions as deemed appropriate by Virtusa Management, Human Resources, and the Legal Departmentof Virtusa.

I understand that:

I agree that am accountable for any consequences or any misuse of the Virtusa/Client information assets. I further undertake to abide by this Asset Security Terms as part of joining the company and my continuing employment in Virtusa, irrespective of movement across various roles & responsibilities and to any other locations. Further I irrevocably agree and undertake that the company reserves the rights to take any and all appropriate remedial measures for any loss arising out of misuse or abuse of company information or information related devices / assets under any and all circumstances and with no notice.

I hereby agree and undertake to fully indemnify, defend and hold harmless Virtusa, including its respective directors, officers and keep them indemnified from and against any third-party claim, demand, losses, liabilities or expenses of any nature and kind whatsoever , including without limitation, all reasonable legal and litigation costs and expenses (including reasonable attorney's fees) as incurred as a result of acts, omissions, negligence, misconduct or breach of obligations by me under this Asset Security Terms.



Employee Signature
IP Address: 2401:4900:6345:53f8:f0cc:bf9c:8c16:1b84
Name: Totakura Madhu Shantan **Date of Signing:** 13-08-2024