निदेशालय
DIRECTORATE OF INCOME TAX (SYSTEMS)
, — , I—2,
ARA Centre, Ground Floor, E-2, Jhandewalan Extension,
New Delhi-110055

ITBA Internet Instruction No.2

F. No. System/ITBA/Security/2020-21/ Dated: 04-05-2020

1. Recommended best practices and responsibility of officers accessing ITBA applications over VPN :

i) All Information assets of the Department must be used for business purposes only by its authorized users. All users must adhere to safe usage practices that do not disrupt business or bring disrepute to the Department.

iii) Users are responsible to ensure that confidential, secret and top secret information asset is not stored on vulnerable machines.

ii) Users must ensure that all important information possessed by them is password protected and that the password is only shared with people on a need-to-know basis (if required).

iv) Users must not share/ disclose their passwords with other users and third parties. All users are responsible for the activities performed through their login.

v) Users must log out of computer terminal when finished accessing programs, or if left unattended.

vi) Users must not install any software or applications on their computer that is not authorized or not essential to the Department's business.

vii) Users must not alter or change data contained within the Department computer systems in any way unless authorized to do so.

viii) Users must not disclose any organizational data to anyone inside or outside the organization, unless authorized to do so.

ix) Users must not install unauthorized hardware like a modem, removable media, boot device, etc. which could be used for either gaining access to the Department computer system or copying data from the system.

x) User should not share departmental laptop with anyone else.

xi) User should secure laptop with password.

xii) User should ensure that microphone and video/camera is on OFF mode and enabled only on explicit action by the User.

xiii) User should keep browser up-to-date.

xiv) User should not click on links from unknown sources.

*) User should not visit unknown or unauthorized websites.

xVi) User should not visit non- work related websites from official system. Few examples stated below:

- Social Media Platforms
- E-commerce websites
- Video or music sharing ,downloading orviewing websites

xvii) Be Careful with What You Download.

XVuI) Websites starting with https:// instead of http:// have an extra layer of browser security because they encrypt your data. So always verify the URL of the site that you visit

xix) User should check if lock next to https is green, this makes sure User is on correct web server which has been verified.

xx) User should take periodic backup of data

xxi)User should not disable antivirus, should keep anti-virus updated and scan the laptop

xxii)periodically to ensure it is free from malware