OFFICE OF THE COMMISSIONER OF CUSTOMS (IMPORT)
JAWAHARLAL NEHRU CUSTOM HOUSE, NHAVA SHEVA,
TAL: URAN, DIST: RAIGAD; PIN- 400 707 (M.S.)

F.No. EDI- 35/2009 JNCH Date: 25 .06.2009

STANDING ORDER NO.28 /2009

Sub : Security of Password by ICE Users Reg.

Attention of all Officers of this Custom House is invited to Standing Order No. 36/2006 dated 22.08.2006 and Directorate General of Systems & Data Management�s instructions vide F.No. IV (26)/47/2009-Systems/2289 dated 25.05.2009 regarding �security of password by ICES users and general guidelines on IT security�.

2. It is once again reiterated to follow the Standing Order NO. 36/2006 strictly.

3. It has been observed that the adherence to these guidelines has been lax and instances of misuse of systems by unauthorized persons are traceable to the disregard shown by officers in protecting their password.

4. It is learnt that the Directorate of Systems has commenced the rollout of the IT Consolidation Project beginning with the Automated System for Central Excise and Service Tax (ACES), ICEGATE and the corporate mail facility on Lotus notes.� Shortly, ICES and other applications such as Data Warehouse would be launched.� For access to applications all officers would be issued with a single sign-on (SSO) identification that would allow them to use applications which they are entitled to.

5. The Consolidation project also seeks to implement the ISO 27001 standard for security Assurance in respect of the equipment, processes and applications under its ambit.� For this purpose, the Directorate is currently in the midst of working out a comprehensive security policy, guidelines and detailed procedures on each area of IT security.� However, there would be several computers and applications (locally developed) in field formations that would continue to remain outside the ambit of Consolidation.� In view of this, the following general set of guidelines on end user security is prescribed for strict compliance of all officers.�

6. These general guidelines apply equally to all IT infrastructure and processes irrespective of their application domains i.e. they apply equally to IT infrastructure and process outside the Consolidation project.� These guidelines also contain information relating to appropriate use of Internet in offices using official networks.

I. Desktop and Network Security

DOS:

1. Lock your desktop/laptop using (Ctrl + Alt + Del) while away from your desk.� It is an absolute must.� Unless the Clear Screen Policy is implemented in this manner, every time you leave your desktop unattended, any unauthorized person may copy or modify your data or carry out transactions on your behalf.� You will be solely responsible for any consequences of your negligence.
2. Log off from Applications when way from your terminal.
3. Shutdown desktops/laptops and Monitors while leaving office and do not delegate this to any other persons.
4. Ensure that Desktop is updated with latest Anti Virus version.� Virus, worms and Trojans not only affect your machine but also the entire network, both local and wide area and can paralyse work of other officers.� Any machine found to be virus infected will not be allowed to be connected to CBEC�s data centers.
5. Ensure all software installed on any desktop is licensed software.� All Asstt/Dy. Commissioners should undertake a review to ensure that only licensed software is being used in their formations.
6. Back up your files on a regular basis on authorized media.� This means that you should not use private media to backup official files.� Please remember in the event of a virus attack, all important documents may be lost unless backed up in time.
7. All media including software licenses must be properly labeled and indexed in a guard file.� This would enable you to restore any machine or device from software failures.
8. All such authorized media must be kept securely to prevent any unauthorized access.� This is important in checking that legitimate software bought by you is not reused by unauthorized persons.

DON�TS:

1. CD/DVD or USB enabled devices should not be brought within the office premises, unless required for any specific official purposes.
2. Do not make your personal folder share-able over network unless there is compelling business need.
3. Do not install unauthorized software � unlicensed software, freeware, games, etc. Very often such software contain backdoors and Trojans that can cause leakage of password and other sensitive data.
4. Do not allow your service provider to carry away licensed software CD.� Any work done by the service provider should be supervised by you or an authorized representative and all media used by the provider should be returned and accounted for.
5. As indicated above, in case of any violation of these instructions, such as official data being found on private devices the onus to establish that the deviation was for official reasons would be on the concerned officer.� Utmost care is therefore advised while copying data across different media.� To the extent possible, formal mechanisms for taking approvals should be in place.

II.� ����� Password Management

DOS:

1. Change the default password after first login.� Very often the first password is known to the system administrator and other super users and it is mandatory that you change it immediately.
2. Create passwords consisting of alphanumeric and special characters.� When used in combinations of alphanumeric and special characters, it becomes much harder to crack the password even through brute computing force.
3. Ensure that the length of the Password should be minimum of 8 characters.
4. Change your Password every 30 days or earlier as per system norms. In case of local applications, System managers are advised to ensure that the Operating System makes it mandatory for users to change passwords.
5. Ensure that the new password should not be same as the latest 3 passwords.
6. Consider using a phrase or a song title as a password.� For example, �Somewhere Over the Rainbow becomes �SW0tR8nBO�

DON�TS:

1. Do not share your password with anyone, howsoever friendly or close the person may be to you.� Please also beware of any mail asking for your password or any person purportedly calling from helpdesk any/or vendor agencies under the consolidation project and asking for your password.� In all such cases, consult the Directorate of Systems through your local System Manager.
2. Do not let others watch you enter the password.� Please advise persons near you to look away when you enter passwords or wait till they leave the room before you enter the password.
3. Do not write your password openly anywhere, including your diary, mobile phone or slips in your wallet.
4. Do not enable the �Save Password� option if prompted to do so either by browser or any local software.� You may encounter this while logging on to mail servers including Google and Hotmail or to applications.� Once you enable this, in future anyone can log into your account without having to enter the password.

III.������ Internet Security

DOS:

1. Use Internet only for official business purposes.� Please remember that when you use the Internet for entertainment or any other unofficial purpose you are wasting Government resources and time; and also hampering other legitimate users from accessing the Internet for official work.� You would also open up a big source of malware since many entertainment and general purpose sites are the source of such software.
2. Ensure all the documents downloaded from the internet are scanned for viruses before being opened.

DON�TS:

1. Do not download files of following extension : exe, .mpeg, .mp3, avi, .scr, hqx, .qt, sit, cbl, .rm, .wmv, .dat files
2. Do not access entertainment, financial brokerage, pornographic, social networking, peer to peer sharing sites like kazaa, torrent, etc.
3. Do not upload or download unauthorized software like freeware/games.
4. Do not provide personal, sensitive information to any unknown web-site.
5. Do not access social networking sites such as Facebook and Orkut.

6. Do not use the automatic logon/store passwords feature in websites.
7. Do not depend on free information obtained through the Internet through sites such as Wikipedia.� This is because the timeliness, accuracy, author bias and continued availability of such information are not reliable.

IV.������ E-mail Security

DOS:

1. The Directorate of Systems would be providing official email accounts to all officers shortly.� Wherever such official mail accounts have been provided, you should use the account for official purposes only.� All mails would be archived in CBEC�s data center and mails entering and leaving CBEC�s network would be subjected to scans.
2. Open mails from known senders only.
3. Ensure that the attachments are scanned for viruses before opening.

DON�TS:

1. Don�t open mails from unknown persons, especially those that carry attachments that you were not expecting.
2. It is reiterated that you must not open attachments with a suspicious file extension (*.exe, *. vbs, *.bin, *.com, or *.pif).
3. Don�t open a message that directs you to click on a web link.
4. Don�t open E-mail with unusual topic lines, like: �Your car?� Oh! Nice Pic! Family Update! Very Funny!�

7.�������� All concerned are directed to follow the above guidelines scrupulously, and disregard of these instructions may invite disciplinary actions. In case any violation of these guidelines is observed, the onus to establish that the deviation was for official reasons would be on the concerned person.

(A. K. DAS)
COMMISSIONER OF CUSTOMS (IMPORT)
JNCH, NHAVA SHEVA.

To,
All the Concerned

Copy to :
1.� The Chief Commissioner of Customs, JNCH, Sheva.
2.� The Commissioner of Customs (EP), JNCH, Sheva.
3.� The Commissioner of Customs (Appeals), JNCH Sheva.