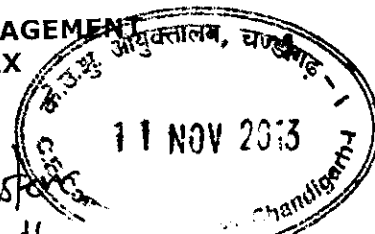




DIRECTORATE GENERAL OF SYSTEMS & DATA MANAGEMENT
CUSTOMS, CENTRAL EXCISE & SERVICE TAX
4th & 5th FLOOR, HOTEL SAMRAT,
KAUTILYA MARG, CHANAKYA PURI,
NEW DELHI- 110 021



IV(26)/104/2008-Systems

*PL discuss
SMT
PL code
1/1/11*
Dated: 28.10.2013

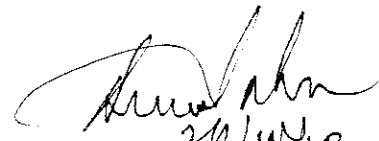
To,

All Chief Commissioners of Customs / Central Excise/Service tax
All Commissioners of Customs / Central Excise/Service tax

Sub: Instructions for User Access Management and Information Security at field formations redg.

Please refer to earlier letter no. IV(26)/104/2008-Systems/436 to 593 dated 23.02.2012 in respect of Validation of User Template and OID-SSO for CBEC & Non-CBEC Users at Customs/ Central Excise locations and Directorate along with its attachments. In that context, the following points may please be noted.

- 20
2. CBEC is a ISO 27001 standard compliant organization in respect of its centralized IT infrastructure. This globally accepted standard for Information Security, places great emphasis on the domain of User Access Management. This makes it imperative that all formations which have personnel accessing the central data centre, monitor and review their users on a regular basis.
 3. Annexed herewith are instructions/ guidelines which all officers may be apprised of. There are additional instructions for the notice of System Managers/ Commissionerate Administrators. Assiduous compliance to the procedures/ instructions in this advisory will help streamline the functioning at the field formations.
 4. It is also informed herewith that this office is about to launch a system ('User Verification tool) for verification of users by Nodal Officers (System Managers/ Commissionerate Administrators). Detailed instructions in respect of the same will follow.


(Arun Sahu) 20/10/13

Director General of Systems

Encl: (A) Instructions to all CBEC officers

(B) Additional Instructions for Local System Manager/Alternate System Managers and Commissionerate Administrators

Instructions for All Officers

1. If you need a SSO ID to access CBEC applications or ICEGATE Email ID or VPN ID, please contact your Nodal Officer (Local System Manger (SM)/ Alternate System Manager (ASM) or the Commissionerate Administrator). ID creation/ modification/ disabling requests to si.helpdesk@icegate.gov.in should be routed through the Nodal officers only. The applicable template should be taken from <http://apps.cbec.gov.in/Citrix/AccessPlatform/auth/login.aspx> or www.cbec.gov.in. In case of issues/ delays in request processing, you may write to cbec.usermgmt@icegate.gov.in
2. CBEC has implemented a '30 days mandatory password expiry policy', hence please change your SSO ID password every 30 days. (detailed instructions are available on <http://apps.cbec.gov.in/Citrix/AccessPlatform/auth/PasswordEnforcementDocument.htm>). The system will display a warning message 7 days prior to the expiry.
3. To change your SSO ID password (on expiry of 30 days from last password change) please follow the steps below:
 - a. Open the link <http://apps.cbec.gov.in>
 - b. Click on the "Change Password" link.
 - c. User has to answer 3 security questions to reset the password.
 - d. To change answers for security questions, user has to click on "Challenge Q&A" link.
4. In case you have forgotten your SSO ID password, please follow the steps listed below to reset the same:
 - a. Go to <http://apps.cbec.gov.in>
 - b. Click on 'Change Password'
 - c. Click on 'Forgot Password'
 - d. Answer 3 Security Questions
 - e. Choose new password-
 - i. *Please note that your password must contain at least 1 special characters (excluding =@&()|\'<>+/? . :}[]\$%#) , 1 lowercase letter, 1 uppercase letter, 1 numeric character and 2 alphabetic characters*
 - ii. *Passwords will expire in 30days from the date of last password change*
5. In case your answers to 'Security Questions' are not set; please contact the SI Helpdesk for getting your password reset. They will verify your details in the systems, in case of any discrepancies noted, please send copy of relevant pages of service book record, through your nodal officer's official ICEGATE Email ID, for record correction.

6. Do not share your SSO ID/ ICEGATE Email ID/ VPN ID login details with anyone. Anyone requiring a SSO/ ICEGATE Email/ VPN ID should send a request in the prescribed template through their nodal officer.
7. Lock your desktop/ laptop while away from your desk. Protect your system with screen saver passwords
8. Log-off from your applications when away from terminals
9. Shut-down your system before leaving office
10. Shred unwanted copies of sensitive documentation
11. Consider scanning paper items and filing them electronically
12. Use the recycle bins for Public documents when they are no longer needed. Empty recycle bin periodically
13. Lock your desk and filing cabinets at the end of the day
14. Protect your system with screen saver passwords
15. Do not do internet surfing on a system connected to the LAN
16. Do not download freeware and shareware on your official PC/ thin client
17. Do not allow your service provider to carry away licensed software CD. Any maintenance work done by service providers should be supervised by CBEC officials
18. Scan all email attachments for viruses before opening them
19. Clean up cache files in the browser and empty recycle bin after use of shared PCs
20. Follow Clear Desk and Clear Screen Policy
21. Do not Click on links embedded in spam mails
22. Do not Use illegal/ unlicensed software and programs
23. Do not Open email attachments from unsolicited sources
24. Never share passwords or other sensitive information in response to an unknown email sender as it could be 'Phishing' attack

**Additional Instructions for Local System Managers/ Alternate System Managers and
Commissionerate Administrators**

The role of Local System Manager (LSM)/ Commissionerate Administrator (Com Admin) is very vital at local level as LSM/ Com Admin is the officer who provides access to various applications to officers depending on location's business needs and also disables access to these applications when an officer is transferred out / retired / promoted or has resigned from service. In recent past, certain security incidents have made it imperative to re-emphasize certain Do's and Don'ts as part of the discharge of duties towards the LSM/ Com Admin role.

Do's

1. All SSO ID/ ICEGATE Email ID/ VPN ID creation requests have to be forwarded to SI Helpdesk (si.helpdesk@icegate.gov.in) by the LSM/ Com Admin through his/ her ICEGATE Email ID.
2. LSM/ Com Admin should verify that all user details in the template, for SSO ID and ICEGATE Email ID, are complete and correct. For e.g. DoB may be verified against the DoB mentioned in the service book or any Government issued ID of the User.
3. LSM/ Com Admin should ensure that correct and latest version of a template is used for any user requests. It is advisable that for new requests templates available on the CBEC website (www.cbec.gov.in) or Citrix Home Page (<http://apps.cbec.gov.in>) at that point in time be downloaded and used as frequent changes are made to these templates based on inputs from various stakeholders.
4. In case a user is transferred out / retired / promoted or has resigned, the LSM/ Com Admin should proactively first revoke the user's application roles and privileges inside ICES/ACES (as the case may be) and only thereafter inform SI Helpdesk for disabling access to application. Many instances have come to notice wherein the user was transferred from location 'A' to location 'B' but LSM/ Com Admin at the location 'A' had not transferred pending tasks in the users' (who is being transferred) queue to another user. Subsequently, the SI Helpdesk received a request from LSM/ Com Admin at location 'B' to map the user to the new location and modify application access. The helpdesk processed the request, after due approvals. Later work at location 'A' was hampered as the pending tasks appeared in the LSM/ Com Admin list against the user transferred out of the location, but the LSM/ Com Admin were not able to assign these tasks to another user. Implement a procedure for monthly review of all system users at your location, as officers retire every month, there are transfers and promotions that entail a change in the user profile and immediate deactivation is required in case of resignations from service
5. If LSM/Com Admin is himself/herself getting transferred out of a location or retiring, he/she should ensure that proper handover of all user issues is done to the alternate LSM/Com

Admin. It should be ensured that the user name and accountability of a generic email account (such as sysmgr.loc@icegate.gov.in), if any, is formally handed over to the incoming LSM/ Com Admin.

6. For all VPN ID requests, LSM/ Com Admin should ensure that desktop details of the desktop on which VPN client would be installed, are provided in the VPN ID template.
7. For all SSO ID and/ or ICEGATE Email ID requests, LSM/ Com Admin should ensure that the Alternate Email ID and Mobile number of the user (s) are provided in the template as the ID and password details would be shared with the user only. In cases where the user does not have either an alternate Email ID or Mobile Number, the ID and password details would be shared with the LSM/ Com Admin and LSM/Com Admin would be responsible for sharing the details with the users and ensuring that passwords are changed upon first login.

Don'ts

1. LSM/ Com Admin should not share his / her ID and password details with anyone.
2. LSM/ Com Admin should not share sensitive CBEC/ User related information through unprotected flash drives.
3. LSM/ Com Admin should not delegate their responsibilities related to user access management to any officer (LSM may delegate responsibilities to except Alternate LSM).