Republic of the Philippines
Department of Finance
BUREAU OF CUSTOMS
1099 Manila

CUSTOMS MEMORANDUM ORDER
NO. 34-2015

Subject: **USE OF BUREAU OF CUSTOMS ICT ASSETS, DATA, INFORMATION AND NETWORK/INTERNETWORKING AND INTRANETWORKING FACILITIES**

I. OBJECTIVE

To lay down the policy on the utilization of BOC ICT assets and facilities and institute the necessary controls to prevent unauthorized use thereof, as well as, to provide for the list of prohibited acts and their equivalent administrative offenses to ensure the security of the said assets and facilities and the integrity of the data and information contained therein.

II. SCOPE

This memorandum order shall cover the use of ICT facilities and resources of the BOC by the Bureau's organic personnel, as well as, all other personnel contracted by the BOC. This will also cover third party implementation partners and all persons which connect or use the ICT resources of the BOC.

III. GENERAL PROVISIONS

1. The ICT network facilities and resources of the Bureau shall be used strictly for official functions and other work-related activities.

2. The Commissioner or the Deputy Commissioner for MISTG may approve the use of network resources beyond the scope of the immediately above paragraph under the following conditions:

   a. The use is necessary in the interest of national security; and/or,

   b. The utilization is essential in protecting the interest of the Bureau.

3. Commission of any of the acts listed herein, as well as, any other act in violation of III.1 shall, after proper proceeding, be subject to the penalties commensurate to the offense committed.

IV. ADMINISTRATIVE PROVISIONS

1. There shall be an Oversight Committee to administer and ensure compliance to the policies laid down herein. The Oversight Committee shall be headed by the Deputy Commissioner, MISTG, with the Deputy Commissioners for Enforcement Group (EG) and Intelligence Group (IG) as members.

2. The Oversight Committee shall be assisted by a Secretariat to be headed by the Chief, Systems Management Division, with personnel from the said division, Intelligence Division, CIIS, and Customs Police Division, ESS, as members. The

members shall be designated as such by the Commissioner in such number as may be necessary for the effective implementation of this memorandum.

3. The Oversight Committee shall, from time to time, submit to the Commissioner plans and programs to effectively implement the provisions of this memorandum.

4. Upon receipt of any complaint or report of commission of any of the acts prohibited herein, the Head, Secretariat, shall assign a member to conduct an initial fact finding inquiry as to the veracity of the complaint or report. In case of finding of probability of the commission of the prohibited act/s, the Secretariat shall submit its report and recommend to the Oversight Committee the referral of the case for formal investigation before the Investigation Division, CIIS.

5. The Oversight Committee, may, on its own, refer a case for formal investigation before the Investigation Division, CIIS. In all cases of referral for investigation, the Oversight Committee shall furnish the Office of the Commissioner a copy of the said referral.

6. The finding of administrative liability shall not preclude the Bureau from filing the necessary criminal action, as warranted by the facts and evidence.

7. For purposes of this memorandum, listed hereunder are prohibited acts and their equivalent administrative offense

ICT Resources Usage & Network Security Offenses	**Equivalent Administrative Offense**
1. Commercial Use - Use of BOC ICT Resources for commercial purposes and product advertisement for personal profit	Grave Misconduct
2. Religious or Political Lobbying - Use of BOC ICT Resources for religious or political lobbying. Engaging directly or indirectly in partisan political activities by one holding a non-political office	Conduct Prejudicial to the Best Interest of the Service
3. Copyright Infringement - Reproduction, duplication, transmission of copyrighted materials using unlicensed software.	Grave Misconduct
4. Criminal Use - Using the resources for criminal activities	Grave Misconduct
5. Wiretapping and Unauthorized Traffic Capture - the unauthorized rerouting or capture of traffic transmitted over the voice or data network	Grave Misconduct
6. Stealing - Stealing of information resources both hardware or software or any part of the network resource	Grave Misconduct

7. Concealing Access - concealing one's identity or masquerading as another user to access the information resource, send/receive, process, modify or store data on the ICT Resources	Grave Misconduct
8. Unauthorized Password Disclosure/ Use - disclosure of a user password/PKI-protected account or making the account available to others without the permission of the System Administrator	Grave Misconduct
9. Unauthorized Intrusion - attempts to disable, defeat or circumvent any BOC ICT security policy. Unauthorized access to another computer or network thru decrypting, hacking, hijacking, spoofing, etc.	Grave Misconduct
10. Unauthorized access of other accounts or files within or outside BOC's computers and communication facilities without proper authorization	Simple Misconduct
11. Unauthorized copying, renaming or changing information on files/programs that belongs to another user unless the said user gave permission	Simple Misconduct
12. Unlawful messages – Use of BOC ICT electronic communication facilities (such as email, talk, chat or systems with similar functions) to send fraudulent, harassing, obscene, threatening or other offensive messages	Grave Misconduct
13. Offensive Prohibitive Materials - use of computers, printers, electronic mail, data network and other related resources to produce, disseminate, store or display materials which could be considered offensive, pornographic, racially abusive, libelous or violent in nature	Grave Misconduct
14. Prohibited Materials - Using or encouraging the use of materials that includes instructions to gain unauthorized access (e.g. Hacker's Guide)	Grave Misconduct
15. Unauthorized reading of email or private communications of other users, unless otherwise requested to do so by said users	Simple Misconduct
16. Misrepresentation in sending e-mail messages	Grave Misconduct
17. Systems Software and Hardware Removal - Unauthorized removal or modification of system software and hardware on any of the BOC ICT Resource	Grave Misconduct

18. Damaging/Vandalizing - Damaging or vandalizing any of the Bureau's Resource including but not limited to all the facilities, equipment, computer files, hardware and software	Simple Misconduct
19. Unauthorized manipulation/ changing of the BOC ICT Network architecture or setup	Grave Misconduct
20. Software and Hardware Installation - Unauthorized installation of software and hardware on any of the BOC ICT Resources	Violation of Reasonable Office Rules and Regulations
21. Not cooperating with any investigative process in line with computer, network or system abuse	Simple Misconduct
22. Disclosure of BOC Confidential Information - Transmission of information without authority and proper security clearance. Disclosing or misusing confidential or classified information officially known to him/her by reason of his/her office and not available to the public to further his/her private interest to give undue advantage to anyone or to prejudice the public interest	Grave Misconduct
23. Access to lewd sites - A user should not view, transmit, retrieve, save or print any electronic files, images or text which may be deemed sexually explicit or pornographic	Violation of Reasonable Office Rules and Regulations
24. Changing of IP Addresses, Network configuration, adding or connecting unauthorized equipment/device without the prior written approval from MISTG-authorized personnel	Violation of Reasonable Office Rules and Regulations
25. Personal Entertainment - No ICT resource must be used for playing any computer game whether individually or in a multiplayer setting, to be used in watching movies thru VCDs, DVDs and other media	Violation of Reasonable Office Rules and Regulations
26. Failure to report use of ICT resources for personal entertainment	Violation of Reasonable Office Rules and Regulations
27. Making of false unsubstantiated accusations in filing a report	Simple Misconduct
28. Any other unauthorized use of the ICT facilities, equipment and/or resources.	Violation of Reasonable Office Rules and Regulations

V. REPEALING CLAUSE

All Customs Memorandum Orders, rules and regulations inconsistent herewith are hereby superseded, repealed or amended accordingly.

VI. EFFECTIVITY

This Order shall take effect immediately."

ALBERTO D. LINA
Commissioner

Bureau of Customs
ALBERTO D. LINA
Commissioner
15-01767

SEP 24 2015