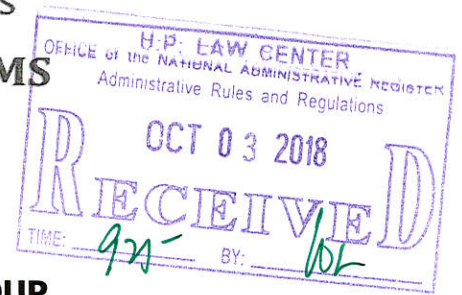




REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF FINANCE
BUREAU OF CUSTOMS

(E)



INTERNAL ADMINISTRATION GROUP
CENTRAL RECORDS MANAGEMENT DIVISION

October 03, 2018

The Director

Office of the National Administrative Register (ONAR)
UP Law Center Diliman, Quezon City


Sir/Ma'am:

Transmitted are three certified true copies and soft copy (word format in compact disc rewritable) of the following Customs Memorandum Order, to wit:

CMO 15-2018: E2M USER ACCESS POLICY.

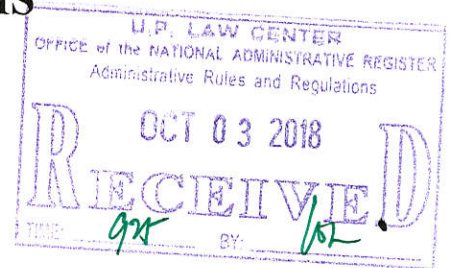
Thank you.

Very truly yours,


GLADYS C. CABUGAWAN
for Chief, CRMD



Republic of the Philippines
Department of Finance
BUREAU OF CUSTOMS



CUSTOMS MEMORANDUM ORDER (CMO)

NO. 15 - 2018

SUBJECT: E2M USER ACCESS POLICY

Introduction. It is essential that access to, and use of, the BOC's applications, systems, and data are properly secured and protected against information security related threats and abuses.

Protecting access to the E2M customs systems and applications is critical to maintaining the integrity of its data and to prevent unauthorized access. This policy defines the Bureau of Customs' (BOC) expectations of users who have been granted access to the E2M systems and other customs applications.

Section 1. Objectives.

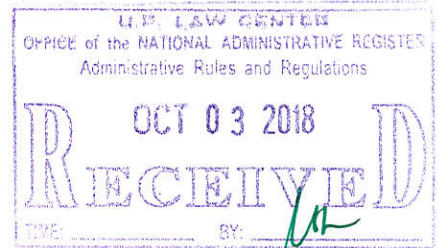
- 1.1. To ensure that the BOC has adequate controls to restrict and regulate access to its systems, applications and data to authorized users only;
- 1.2. To prescribe the standard procedures for managing the access to BOC's E2M system and other related applications;
- 1.3. To instill user accountability and responsibility of accessing the BOC's E2M system, applications and data;
- 1.4. To account and monitor all access granted to all users of BOC systems, applications, and data; and
- 1.5. To conduct regular audit, evaluation, and provide recommendations to address any weaknesses and vulnerabilities in access controls, as the case may be.

Section 2. Scope.

- 2.1. This memorandum order shall cover all persons with access to the BOC's E2M system, its related applications and the data stored and processed in and through it, including:
 - (a) BOC organic personnel;
 - (b) BOC personnel under a contract of service or consultancy agreement;
 - (c) BOC accredited VASPs (Value Added Service Providers) and their respective employees and agents
 - (d) Other Government Agencies (OGA) and its employees given authorized access to the E2M system and its related applications; and
 - (e) All other persons that connect to or access the E2M and its related applications.

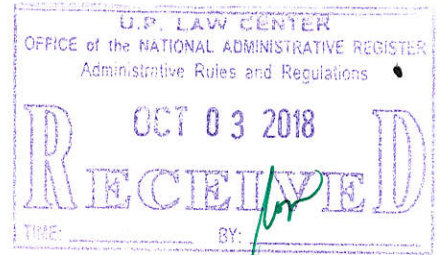
Certified True Copy

Raquel G. De Jesus
SVCOO
CRMD - BOC



Section 3. Definitions.

- 3.1. **Access Privileges** – refers to system permissions associated with an account, including permissions to view, edit or retrieve data, to process transactions, create or change settings, etc.
- 3.2. **Account Activation** – refers to the enabling of access to the system or reviving of a user's access if previously deactivated
- 3.3. **Account Deactivation** - refers to the suspension or temporary disabling of a user account and the accompanying access privileges
- 3.4. **Account Revocation** - refers to the cancellation or termination of a user account
- 3.5. **Account Restriction** - refers to the limitation or change of access privileges of a user account
- 3.6. **Administrator Account** – refers to a user account with privileges that have advanced permission that is necessary for the administration of the system. This account can create or modify settings, view activities, and edit access privileges of other user accounts.
- 3.7. **Regular User Account** – refers to accounts that are for viewing purposes only
- 3.8. **Required training** – refers to training that is commensurate or needed to perform the assigned roles or duties.
- 3.9. **Security and Access Matrix** – refers to a centralized registry of BOC systems with the list of users' positions, functions and their corresponding access rights as approved by authorized MISTG officers.
- 3.10. **Temporary Access** - refers to a user access granted based on special designation or function but shall be limited in time and scope.
- 3.11. **Terms of Use (TOU)** – refers to a contract between an individual granted a user account and the BOC providing for the responsibilities of the user to protect the integrity of the account and any confidential information when the said person has been exposed to such information.
- 3.12. **User Access Request Form (UARF)** – refers to a form to be filled-out by the party requesting access to the E2M and can be secured from MISTG Site personnel or boc.cares@customs.gov.ph or at www.customs.gov.ph (also referred to as the *Log-In ID Request Form*)
- 3.13. **MISTG** shall refer to the Management Information Systems and Technology Group created under E.O. No. 463, series of 1998.



Section 4. Administrative Provisions.

- 4.1. The granting of user's access shall be limited to specific, defined, documented and approved applications and levels of access rights shall be based on the assigned role or function. The users shall only receive access to the minimum applications and privileges required to perform their job-related functions.
- 4.2. User accounts logged in to the E2M system but remain idle for 30 minutes shall be logged off automatically by the system.
- 4.3. The password policy for E2M user accounts shall be set by MISTG, with the following minimum standards:
 - (a) frequency of password changes shall be not less frequent than once a month
 - (b) password complexity (minimum of 8 characters, with upper case, lower case, and number)
- 4.4. The Terms of Use (TOU) to be signed by persons granted E2M access shall include provisions ensuring compliance with RA 10173 or the Data Privacy Act of 2012 and its implementing guidelines.

Section 5. Request for E2M Access.

- 5.1. The users requesting for systems access shall fill-out the UARF and attach the following documents:


BOC Personnel

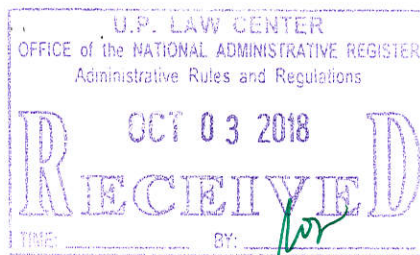
- (i) Customs Personnel Order (CPO) issued by the Commissioner of Customs designating the BOC personnel to a position requiring E2M access
- (ii) Certificate of Assumption of Duty
- (iii) Certificate/s of Training related to the requested access
- (iv) Approved and Signed Terms of Use
- (v) Endorsement or Clearance from the District/Port Collector or Deputy Commissioner where personnel is assigned
- (vi) For non-operations personnel (IG/EG), the request for access must be with the endorsement of the Deputy Commissioner concerned
- (vii) For personnel under the Office the Commissioner, the request for access must with the endorsement of the Commissioner or his Chief of Staff
- (viii) For BOC personnel under Job Order or Contract of Service, request for access must be made by the immediate superior who must be an organic BOC employee

For Other Government Agency (OGA) Users

- (i) Endorsement from Head Office or immediate Supervisor

Certified True Copy


Raquel G. De Jesus
SVCOO
CRMD - BOC



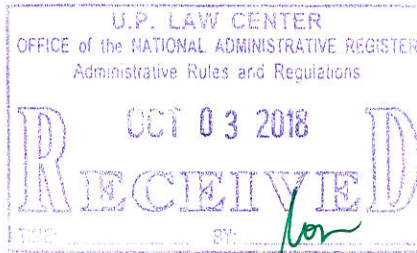
Certified True Copy


Raquel G. De Jesus
SVCOO
CRMD - BOC

- (ii) Justification of access requested
 - (iii) Certificate/s of Training related to the requested access
 - (iv) Approved and Signed Terms of Use
- 5.2. For BOC operations personnel, the documents above together with the signed and filled out UARF, shall be submitted to the MISTG site personnel for compliance check. Once the request is deemed compliant, the MISTG Site Personnel shall sign the UARF and forward the complete set of documents to the Systems Management Division (SMD).
- 5.3. For BOC non-operations personnel, or personnel under the Office the Commissioner, or those belonging to OGAs, the documents shall be submitted directly to the SMD.
- 5.4. The authorized email domain to be used is @customs.gov.ph in accordance with Section 5.1 of CMO 3-2016. Use of e-mail accounts with said domain for official duties is a mandatory requirement per Section 5.2 of CMO 3-2016. If the user has no BOC email account, they must secure one through the MISTG Site personnel.
- 5.5. For non-organic BOC personnel, the account user name in E2M must clearly indicate such status, i.e., (COS_AB.Cruz@customs.gov.ph).
- 5.6. For non-BOC personnel (like OGA users), user account details shall be forwarded by MISTG to their official work email address. Use of free email addresses such as @gmail.co, @rocketmail.com, or @yahoo.com is prohibited.

Section 6. Approval of E2M Access.

- 6.1. The Deputy Commissioner of MISTG is the approving authority to grant user's access to the BOC's E2M system and its related applications.
- 6.2. A request for temporary access should be justified by the Head of Office and MISTG Site personnel. Temporary access should be limited to three (3) months and subject for renewal if the need for extension is justifiable.
- 6.3. For BOC personnel under Job Order or Contract of Service, the grant of E2M user access shall be under the condition that the accountability for the use of the E2M account is shared between the named user and his/her immediate superior who is an organic BOC employee.
- 6.4. If the request is approved, the Deputy Commissioner of MISTG shall endorse the CSW together with the filled-out UARF and the attached documents to the Technology Support Division (TSD) for the creation of the E2M user account.
- 6.5. TSD shall inform the MISTG Site personnel to guide the user to change the initial password. Changing of initial password shall be the responsibility of the user to ensure security of access.



Certified True Copy

Raquel G. De Jesus
SVCOO
CRMD - BOC

- 6.6. TSD is the repository of all documents of processed UARF and can be retrieved anytime for verification or audit purposes.

Section 7. Restriction, Deactivation and/or Revocation of E2M Access.

- 7.1. User accounts may be restricted, deactivated or revoked, at any time without prior notice, due to the following:
- (a) system inefficiencies requiring removal of E2M access, as recommended by the TMS Director;
 - (b) when there is reasonable ground to suspect misuse of access; or
 - (c) Violation of any terms of use or any existing rules and policies affecting E2M access and usage.
- 7.2. In addition to the instances in Section 7.1., the following circumstances shall be grounds for Account Deactivation, without need of prior notice:
- (a) leave of absence;
 - (b) suspension from work due to administrative, civil or criminal case pending before any court, tribunal or any government office; or
 - (c) inactivity for a period to be determined by the MISTG Deputy Commissioner.
- 7.3. User accounts that have been deactivated shall secure approval from their immediate superior before requesting for re-activation.
- 7.4. In addition to the instances in Section 7.1., the following circumstances shall be grounds for Account Revocation, without need of prior notice:
- (a) retirement;
 - (b) resignation;
 - (c) termination of contract from BOC; or
 - (d) change of functions due to transfer of assignment.
- 7.5. Deactivation, revocation, restriction and/or re-activation of a user account shall be with approval of the Deputy Commissioner of MISTG, who shall instruct the TSD to carry out the corresponding action.
- 7.6. Restrictions on accounts, with respect to the extent and duration, shall be determined on a case-to-case basis in accordance with the circumstances.
- 7.7. The Administrative Officer of different ports, MISTG Site personnel and Human Resource Management Division (HRMD) are obliged to submit a list of retired, resigned, terminated, suspended or transferred employees to the Deputy Commissioner of MISTG.
- 7.8. Existing user accounts and access rights shall be reviewed at least every three (3) months to detect dormant accounts and accounts with excessive privileges. Examples of accounts with excessive privileges include:

- (a) An active account with access rights for which the user's roles and responsibilities do not require access;
- (b) System administrative rights or permissions (including permissions to change the security settings or performance settings of the system) granted to a user who is not an administrator; and
- (c) Unknown active accounts.

7.9. E2M access shall be subject to continuous monitoring by the MISTG through the Technology Management Services (TMS). The TMS Director shall make periodic check-ups and report to the MISTG Deputy Commissioner and the BOC Commissioner, any observed activities that appear irregular, such as but not limited to:

- (a) use of virtual private network (VPN);
- (b) accessing account outside authorized work hours;
- (c) excessive use of E2M access; or
- (d) use of E2M access in excess of two (2) hours for non-operations personnel.

Section 8. Sanctions.


Those found to be in violation of the terms of the user access or the provisions indicated in this Order shall be subject to the appropriate administrative sanctions, including civil and/or criminal liability.

The right and prerogative of the BOC to restrict, suspend, or revoke a user's E2M access shall be independent of and shall not be contingent on the pendency or outcome of any administrative, civil or criminal proceeding.

Section 9. Repealing Clause. This CMO repeals other previously issued CMOs which are inconsistent with the provisions here stated.

Section 10. Effectivity. This Order shall take effect immediately.

Certified True Copy



 Raquel G. De Jesus
 SVCOO
 CRMD - BOC


 ISIDRO S LAPENA, PhD, CSEE
 Commissioner



18-17449

SEP 28 2018

