MASTER COPY

Republic of the Philippines
Department of Finance
Bureau of Customs
Manila

January 18, 2016

CUSTOMS MEMORANDUM ORDER
NO. 3 - 2016

Subject: **E-Mail Policy for the Bureau of Customs**

1.0 General Policy

Pursuant to CMO 34-2015, the Electronic Mail (E-Mail) accounts shall be provided to all officials and employees of the Bureau of Customs (BOC) to serve as the official electronic communications facility for use in operations and in officially communicating to the general public.

To ensure that risks are minimized from either intentional or unintentional misuse of the e-mail service, this E-Mail Policy is hereby being enforced for the exchange of information through e-mail.

The use of personal/publicly hosted/freely acquired email accounts in communicating with any person concerning official BOC matters will not be regarded as official communication not having the same functional equivalence of a signed physical document as provided in RA 8792. The use of personal email accounts for official communication are disallowed.

This policy shall ensure that the use of this system does not infringe on the rights of government employees and citizens pursuant to the provisions detailed in RA 10173; is compliant with the provisions set forth in RA 9470; is not used for purposes prohibited under the laws, rules and regulations of the country; and does not legally compromise the Government of the Republic of the Philippines.

2.0 Objectives

2.1 To establish and enforce guidelines on the proper use of the BOC E-mail Service;

2.2 To promote e-mail usage and awareness of the benefits of a paperless communication system; and

2.3 To provide the basis for appropriate disciplinary action on the prohibited use of the e-mail.

3.0 Scope

3.1 The provisions of this policy shall apply to all officials, regular, and contractual employees of the Bureau of Customs.

3.2 It shall apply to all communications and exchanges, whether internal or external, within or outside BOC, using the BOC E-Mail Service. This policy shall also apply to any other acts using features or services provided by or attached to an e-mail.

3.3 It shall also apply to the use of the e-mail accessed through various devices including, but not limited to, computers, tablets and mobile phones.

4.0 Definition of Terms

4.1 Account Holder – refers to any of the following:
(a) BOC officials and employees; or
(b) Individuals authorized by the Commissioner of Customs to use the BOC E-Mail Service for a specific purpose and duration.

4.2 Attachments – textual, graphical, visual, audio or executable files that are attached in e-mail messages.

4.3 Bulk Mail – an e-mail message sent to a large list of recipients.

4.4 MISTG Deputy Commissioner – a person responsible for information systems planning and implementation of the BOC strategic direction in information and communications technology governance and policy enforcement.

4.5 E-mail – refers to the exchange of digital messages through a network using software and servers. This would include accounts that have the following features: address book, calendar, task, real-time backup and restore, clustering/high availability, multi-tenancy, domain administration and role-based delegation, community support.

4.6 Counterfeit or Forged e-mail – e-mail account that makes use or may contain invalid or forged headers, invalid or non-existent domain names or other names that are deceptive.

4.7 E-mail Account Administrator – a person in charge of the administration of the agency e-mail account.

4.8 Internet – a system of linked computer networks that facilitates data communication services, such as e-mail.

4.9 Log-in – an operation that enables the Account Holder to access the mailbox, using an officially issued username and password or other mechanisms to gain access to the E-mail Service.

4.10 Log-Out – an operation that terminates access to the E-mail Service to prevent unauthorized access.

4.11 Mailbox – a function unit that contains stored messages for a specific Account Holder.

4.12 Mailing List/Groups – a set of people whom e-mails are sent/distributed and made accessible but which will not have its own account inbox.

4.13 Spam – electronic junk mail or unsolicited bulk e-mail that is unrelated to work and not otherwise relevant to be opened.

5.0 General and Administrative Provisions

5.1 The Official Agency E-mail domain shall be **@customs.gov.ph**.

5.2 As a rule, only e-mail accounts using the official domain (Section 5.1) shall be used and regarded as official for electronic mail in the performance of official duties and responsibilities of the employee for email communications between BOC employees, other national government agencies, and with the general public. All email exchanges shall maintain the highest professional standards and shall be bound by the provisions of the Code of Conduct and Ethical Standards for Public Officials and Employees (RA 6713).

All email communications must be digitally signed. As such, all email account holders are required to secure a Public Key Infrastructure (PKI) certificate issued by an authorized Registering Authority (RA) under the Philippine Government Certificate Authority (CA). This is to enforce encryption requirements and establish non-repudiatability of electronic mail communications;

5.3 E-mails not related to the performance of official duties and responsibilities shall fall under Section 6.7 or the Prohibited Use of the E-mail Service and may be subject to administrative sanctions and other actions.

5.4 E-mail Account Holders shall observe E-mail Etiquette in creating e-mails (attached in Annex B).

5.5 The contents of the E-Mail Service are considered confidential government communication and subject in its entirety to the provisions of RA 9470. To protect the confidentiality of e-mail messages, PKI certificates and digital signatures shall be used to encrypt or secure messages.

5.6 Client access to the email service shall strictly use IMAP Protocols.

5.7 All data, information and communication sent, received or archived in the E-Mail Service are the property of the BOC. It is understood that in the use of the BOC E-Mail Service, all messages or files sent through the E-Mail Service may be accessed by the employee's superior, the Commissioner of Customs and other authorized officers for work, administration or disciplinary purposes.

5.9 In case of any formal investigation, or upon demand of the Commissioner of Customs where personal email accounts are used as official BOC-related communication, the Bureau has the right to subpoena all such email account or accounts used in the conduct of BOC related business or to communicate BOC-related data or information.

5.8 All official e-mails shall be archived in accordance with mechanisms and policies issued by the ICT Office or the National Archives of the Philippines as detailed in RA 9470.

6.0 Operational Provision

6.1 Division or Non-Personnel Account

6.1.1 Division or Non-Personnel Accounts shall be provided to divisions, sections, units, projects and the like, and shall be used as a channel of communication between the BOC and the general public.

6.1.2 Heads of divisions, sections, units and major projects shall submit a request for an e-mail account to the Deputy Commissioner, Management Information System and Technology Group (MISTG). Upon approval of the MISTG Deputy Commissioner, the account shall be created by the E-Mail Account Administrator.

6.1.3 The e-mail address shall be named in compliance with Section 6.4.

6.1.4 The Division or Non-Personnel Accounts shall be published in the BOC website as part of its compliance to Republic Act 9485, otherwise known as the Anti-Red Tape Act of 2007.

All division and non-personnel accounts are categorically classified as "no reply" or "do not reply" accounts. All replies to messages sent to division or non-personnel account shall be made using a regular employee email account.

6.2 Employee E-mail Account

6.2.1 Employee E-mail Accounts shall be established and used for official purposes only.

6.2.2 Upon hiring a new employee the Chief, Human Resources Management Division (HRMD) shall submit a request for the creation of an Employee E-mail Account to the MISTG Deputy Commissioner for confirmation/approval.

6.2.4 Upon confirmation of the MISTG Deputy Commissioner of the request, the E-mail Account Administrator shall create the Employee E-mail Account.

6.2.5 The e-mail account shall be named pursuant to Section 6.4.

6.2.6 The E-mail Account Administrator shall provide instructions to the employee on how to access the e-mail account.

6.3 Mailing Lists

6.3.1 Mailing lists or group distribution lists may be created in lieu of division or non-personnel e-mail accounts.

6.3.2 Division heads, project managers, component team leaders or employees who need mailing lists shall write a request to the MISTG Deputy Commissioner containing the following:

6.3.2.1 purpose of the mailing list;
6.3.2.2 desired mailing list name; and
6.3.2.3 e-mail addresses of the employees who shall be included in the mailing list.

6.3.3 The aforementioned request shall be approved/disapproved by the MISTG Deputy Commissioner. If approved, the MISTG Deputy Commissioner shall instruct the E-mail Account Administrator to create the said mailing list.

6.3.4 The mailing list shall follow the naming policy prescribed in Section 6.4 and shall be subject for review every three (3) months.

6.4 E-mail Naming Convention

The naming convention for Office and Employee Account shall observe the following rules:

a. The general syntax of the e-mail address shall include the name of the division / section / unit / project of the BOC followed by the domain @customs.gov.ph.

Sample Office/Project Account:

Division/Office/Project	E-mail Address
Public Information and Assistance Division	piad@customs.gov.ph
National Single Window Project	nsw@customs.gov.ph

b. In case of Employee E-mail Account, the general syntax of the e-mail address shall include the first name of the employee, followed by a period (.) and the last name of the employee, followed by the domain @customs.gov.ph.

Sample Employee Account: ***juan.delacruz@customs.gov.ph***

c. In case of employees with the same first and last names, the employee hired first shall follow Section 6.4. The succeeding employees will have e-mail addresses named from the following options:

i. First name + middle initial followed by a period (.) and the last name, followed by the domain name (juanr.delacruz@customs.gov.ph);
ii. Initial of the first name + middle name followed by a period (.) and the last name, followed by the domain name (jreyes.delacruz@customs.gov.ph); or
iii. Initial of the first and middle names followed by a period (.) and the last name, followed by the domain name (jr.delacruz@customs.gov.ph).

6.5 Passwords

6.5.1 Account Holders shall be responsible for their respective passwords. It must not be written down, stored or shared with other persons.

6.5.2 In cases falling under Annex C, the account holders must disclose their password.

6.5.3 Five (5) consecutive failed log-in attempts will trigger an email to the Administrator for suspicious activity. Google can detect if unauthorized person is attempting to access a user's account, a Login Challenge that asks the person to verify their identity will be presented. This is designed to prevent unwanted access to the account, even if the person has obtained the username and password.

6.5.4 Passwords used must have a specified minimum length of at least ten (10) mixed case alpha-numeric characters.

6.5.5 The password must be composed of a combination of: a) upper case letters; b) lower case letters; c) numbers; or d) any of the following symbols (= ? < > @ # $ * !).

6.5.6 The E-Mail Service shall send out an automatic prompt for a password change every six (6) months or as frequently as may be required or prescribed by the MISTG Deputy Commissioner.

6.6 Prohibited Use of the E-Mail Service

6.6.1 No e-mail shall be sent through the E-Mail Service for purposes outside of the performance of official duties and responsibilities.

6.6.2 E-mail Account Holders are prohibited from accessing, copying or deleting the e-mail of another Account Holder without the consent of the latter.

6.6.3 Account Holders shall not disclose their passwords to other persons, unless BOC requires it for legitimate/valid purposes.

6.6.4 The E-Mail Service shall not be used for the creation or distribution of messages that are disruptive or offensive, including comments or statements about race, gender, disabilities, age, religious beliefs and practices or political beliefs, among others.

6.6.5 The E-Mail Service shall not be used for personal or commercial purposes and for the promotion of business or other matters outside of the BOC.

6.6.6 Sending of bulk mail shall be prohibited unless such bulk mail is formally solicited. Users must send e-mail messages and copies thereof only to those with a legitimate need to read the message.

6.6.7 Attaching files in the e-mail message is discouraged. File attachments shall be implemented through a file sending service, as specified in Section 6.6.

6.6.8 Any document covered by Memorandum Circular No. 78, entitled "Security of Classified Matter in Government Departments and Instrumentalities," issued on August 14, 1964 and amended by Memorandum Circular 196, issued on July 19, 1968, shall only be sent using PKI encrypted e-mail until specific guidelines are issued by the National Security Council, Department of Defense or the Office of the President for e-mail messages.

6.6.9 The use of materials, procedures, devices or technologies that will enable unauthorized access to the E-Mail Service is strictly prohibited.

6.6.10 Any link or attachment of unsolicited or suspicious-looking emails must not be opened.

6.6.11 Authorized users are prohibited from using their E-mail Accounts in registering or joining Social Networking Sites and other list groups that are for personal use in nature.

6.6.12 HTTPS, IMAP, POP and PKI digital certificates shall be used to encrypt or secure the connection. Digital certificates shall be used to authenticate users and the e-mail messages.

6.7 Standard E-mail Signature and Disclaimer

6.7.1 All e-mails shall use a standard E-mail Signature with the following format:

Complete Employee Name
Position / Designation
Unit / Section / Division / Office
Complete Office Address
Telephone / Fax Number
URL

Example:
Juan R. Dela Cruz
Customs Operations Officer 2
Formal Entry Division, Port of Manila
Port of Manila Bldg.
Bureau of Customs
Gate 3, Port Area, Manila
PHILIPPINES 1018
Tel. (632)527-0101
www.customs.gov.ph

6.7.2 All e-mails shall indicate the following disclaimer:

The information contained in this communication is intended solely for the use of the individual or entity to whom it is addressed and other parties authorized to receive it. It may contain confidential or legally- privileged (e.g., copyrighted) communication. If you are not the intended recipient, you are hereby notified that any disclosure, copying, distribution or taking any unauthorized action in relation to the contents of this information is strictly prohibited by law. If you have received this communication in error, please notify the Bureau of Customs immediately by responding to this e-mail. If you are not the intended recipient, you are hereby

instructed to immediately delete this message from your system. The BOC accepts no liability for any damage caused by any virus transmitted by this e-mail. Opinions contained in this e-mail or any of its attachments do not necessarily reflect the opinions of the Bureau of Customs.

6.8 Suspension or Termination of the use of E-Mail Service

6.8.1 The suspension or termination of the Employee E-mail Account shall be implemented: (1) in cases of disciplinary action; (2) when Account Holder transfers from BOC to another agency or to a private company; (3) when the employee retires; or (4) when the employee is declared dead.

6.8.2 In case of suspension or termination of E-mail Account, the Chief, HRMD shall prepare a report stating that the Account Holder can no longer use the E-Mail Service, either permanently or temporarily, as the case may be. The report shall also state the reason for such suspension or termination, which shall be submitted to the MISTG Deputy Commissioner for evaluation.

6.8.3 Upon the confirmation of suspension or termination of E-mail Account, the MISTG Deputy Commissioner shall direct the E-mail Account Administrator to suspend or terminate the e-mail account involved.

6.8.4 When an employee resigns or retires, a 30-day notice shall be given before the Account Holder's access to E-Mail Service is terminated.

6.8.5 When an employee is separated from the service for cause, access to E-Mail Service shall immediately be blocked. After thirty (30) days, the E-mail Account shall automatically be terminated.

All contents of emails shall be perpetually archived and not deleted pursuant to the provisions of RA 9470.

6.9 Spam and Counterfeit or Forged E-mail

In case of occurrences of Spam and Counterfeit or Forged e-mails, the Account Holder shall send to the E-mail Account Administrator a copy of the Spam or Counterfeit e-mail so that an immediate investigation can be done. In submitting a report, the Account Holder shall make sure that the following information are present:

a. The subject line "SPAM" together with the subject of the Spam or Counterfeit e-mail (ex. SPAM: pornography).

b. The e-mail address of the sender of the Spam or Counterfeit e-mail must be in the body of the mail.
c. The complete headers must be sent to the E-Mail Account Administrator. This is done by sending the entire e-mail as an attachment, instead of forwarding the e-mail (See Annex C).

6.10 Scheduled Maintenance

6.10.1 The E-Mail Account Administrator shall inform officials and employees of any scheduled/emergency maintenance of the E-Mail service.

For scheduled maintenance – 5 days in advance or prior to the scheduled maintenance.

For emergency maintenance – 8 hours in advance or prior to the scheduled maintenance.

6.10.2 MISTG shall assist the E-Mail Account Administrator in restoring e-mail files lost during a service interruption.

7.0 Roles and Responsibilities

7.1 Management Information System and Technology Group

7.1.1 Communicate the E-Mail Policy to all authorized users of the E-mail Service.
7.1.2 Establish the E-Mail naming convention as prescribed in Section 6.4.
7.1.3 Provide for the maintenance of the BOC's E-mail Service and technical support.
7.1.4 Updates, patches, bugfixes.
7.1.5 Orient personnel head/administrator/CIO.
7.1.6 Provide administrative and account management support.
7.1.7 Monitor legal agreements related to the service.
7.1.8 Communicate administrative matters to agency CIO.
7.1.9 Regulate and investigate matters relating to spam/counterfeit email.
7.1.10 Issue other policy documents as necessary.

7.2 Internal Administration Group, Human Resource Management Division and the respective Administration Office of all District Ports and Sub-Ports

7.2.1 Ensure that all employees have an official email account.
7.2.2 Posting in accordance with RA 9485.
7.2.3 Compliance with the naming convention.
7.2.4 Store and reproduce relevant information on account holders, as necessary
7.2.5 Provide Functional Training on the proper use of Email;

7.2.6 Reporting in case of termination or suspension.
7.2.7 Compliance by account holder to the terms and conditions.

7.3 Management Information System and Technology Group (MISTG) Deputy Commissioner

7.3.1 Confirm/reject requests for account creation.
7.3.2 Direct administrator to create/suspend/terminate accounts.
7.3.3 Approve/reject policies and/or procedures appurtenant to the use of BOC Email service.

7.4 E-Mail Account Administrator

7.4.1 Assistance to users.
7.4.2 Act on spam.
7.4.3 Administer documentation on the use of BOC email.
7.4.4 Verify that email names comply with email naming conventions.
7.4.5 Create/suspend/terminate user accounts as directed by the MISTG Deputy Commissioner.
7.4.6 Administer procedures in creation/suspension/termination of BOC accounts.
7.4.7 Provide technical support as required
7.4.8 Establish support team.
7.4.9 Inform and update personnel head of temporary service unavailability.

7.4.10 Ensure email is read and acted upon.
7.4.11 Sign NDA covering the BOC Mail.
7.4.12 Develop and implement BOC Mail service operations manual.
7.4.13 Implement email service policy.
7.4.14 Monitor and maintain service availability.
7.4.15 Conduct routine backup.
7.4.16 Period tests of the DRP.
7.4.17 Update email facility software.
7.4.18 Submit usage stats and compliance monitoring every month to the agency head.
7.4.19 Deactivate and archive email of users who have resigned/retired/separated or were suspended.
7.4.20 Ensure proper usage.
Generate email usage reports;
7.4.21 Sign the employee clearance form.

7.5 Authorized Users

All authorized users of the E-Mail Service are required to fulfill the following responsibilities:

7.5.1 To sign the form entitled "Authorized User Acknowledgment Form" provided in Annex A before using the E-Mail Service.

7.5.1 To sign the form entitled "Authorized User Acknowledgment Form" provided in Annex A before using the E-Mail Service.
7.5.2 To be accountable for e-mails emanating from their account.
7.5.3 To report immediately any instance of violation of this E-mail Policy to their immediate supervisor.
7.5.4 To read the E-mail Policy and confirm to the E-mail Account Administrator that he/she has read and understood the said policy and will abide by it.
7.5.5 To provide all information relating to the creation of E-Mail Account and ensure that they are correct.
7.5.6 To make use of E-Mail Service as a means of communication with other employees and the general public.
7.5.7 To keep their respective passwords secure, and to change them on a regular basis as specified herein.
7.5.8 To log-out of the E-Mail Account after using it, and refrain from leaving the account unattended.
7.5.9 To adhere to the e-mail naming convention for Employee E-Mail Account as stated in Section 6.4.
7.5.10 To observe the E-Mail Etiquette in Annex B.
7.5.11 To report immediately any occurrence of spam, suspicious, disruptive, offensive, counterfeit or forged e-mail to the E-mail Administrator.
7.5.12 To undergo an Annual User Awareness Training for the responsible and efficient use of the E-Mail Service. New Account Holders shall undergo the User Awareness Training before being granted access to the e-mail facility as part of their orientation program.

8.0 Penal Provision

8.1 Any reported abuse, misuse or inappropriate use of the E-Mail Service shall be subject to disciplinary action in accordance with the Civil Service Commission's prescribed Uniform Rules on Administrative Cases in the Civil Service (See Annex C for the list of possible Violations and Equivalent Administrative Offenses and Sanctions).
8.2 All disciplinary actions and proceedings shall follow the Civil Service Commission's Uniform Rules on Administrative Cases in the Civil Service without prejudice to the filing in court of any other applicable charges by the aggrieved party.

9.0 Policy Review and Evaluation

This E-mail Policy shall be reviewed and evaluated by BOC at least once a year based on its effectiveness, cost to maintain and impact on technical processes. This policy shall be revised as needed based on newly discovered risks, security incidents involving e-mail or any major changes to the BOC organizational setup or information systems.

10.0 Repealing and Separability Clause

10.1 All issuances, orders, rules, and regulations or parts thereof that are inconsistent with the provisions of this Order are hereby repealed, amended or modified accordingly.

10.2 Must any provision of this Memorandum be declared invalid or unconstitutional, the other provisions not affected thereby shall remain valid and subsisting.

11.0 Effectivity

This Order shall take effect immediately and shall last until revoked.

ALBERTO D. LINA
Commissioner

Bureau of Customs
ALBERTO D. LINA
Commissioner
16-00395

JAN 2 2016

MASTER COPY

ANNEX A:
AUTHORIZED USER ACKNOWLEDGEMENT FORM

As in any written policy, the challenge of effectively and efficiently implementing a policy is in the education of all affected parties. Thus, this document is meant to be signed by the authorized user only after he or she has received the appropriate orientation or education about this document.

I have read and understood the Bureau of Customs E-Mail Policy and agree to abide by it.

I understand that any violation of the above policies and procedures may result in disciplinary action, up to and including termination from government service or termination of contract.

Family Name	
First Name	
Middle Name	
Name Suffix	
Designation	
Division / Unit	
Port / Office	
Official E-mail Address	
Contact Number	

_____
Signature

_____
Date Signed

For any questions or clarifications about this policy, refer them to the Customs E-Mail Account Administrator before signing. By signing, the Bureau of Customs presumes that you have fully understood this e-mail policy and shall adhere to it at all times.

ANNEX B:
PROPER E-MAIL ETIQUETTE

1. Be sure to include a subject line.
2. Consider using a BCC to keep e-mail addresses private or to ensure that the "To:" area of the message remains a small size.
3. Write clear and concise messages.
4. Write short sentences.
5. Avoid double spacing your messages as e-mail requires recipients to scroll through messages without the benefit of highlighting or marking the message as one might on a printout.
6. Use a descriptive subject line.
7. Avoid the use of all capital letters.
8. Avoid using colored fonts.
9. When replying to a message, consider deleting part of the original message to save space on the screen. Retain only the part of the sender's message to which you are responding.
10. Avoid using the Reply To All function as this sends your response to all recipients of the e-mail.
11. Avoid acronyms because not everyone will know their meaning.
12. Use proper grammar and conduct a spell check of your messages.
13. Use simple fonts. Use also a small or compact font to keep the message in a more confined area.
14. Be specific. State terms and conditions clearly to avoid miscommunication, especially when providing information about times, places or people.
15. Leave the address field blank and fill it out last, to avoid sending unchecked or hastily written messages.
16. Do not use unnecessary punctuations.
17. Do not use text messaging shortcuts.
18. Avoid emoticons.
19. Never use slang language.
20. Remain gender neutral.
21. Keep harassment and discrimination policies in mind.
22. Never reply to spam.
23. Ask permission before forwarding.
24. Be cautious when sending attachments.
25. Always use salutations and signatures.

ANNEX C:
HOW TO ATTACH E-MAILS

1. Click the "New Message" button.
2. Click the drop-down menu on the "Attach" button.
3. Select "Mail" from the drop down menu.
4. Select the message to be attached.
5. Fill-up the other fields as necessary, including the recipient's information and the subject field.
6. Click the "Send" button.

ANNEX D:
HOW TO CREATE A SIGNATURE FOOTER

1. Go to "Settings" or "Preferences".
2. Go to "Signature" and enter your new signature text in the box. Use the options to format the texts.
3. After writing the signature of choice, click on the "Save".
4. The signature must appear on all succeeding messages composed by the user.

ANNEX E:
VIOLATIONS AND EQUIVALENT ADMINISTRATIVE OFFENSES AND SANCTIONS

Violation	Offense
Commercial Use – Use of Agency ICT Resources for commercial purposes and product advertisement for personal profit	Dishonesty / Grave Misconduct
Religious Lobbying – Use of Agency ICT Resources for religious lobbying	Conduct Prejudicial to the Best Interest of the Service
Political Lobbying – use of Agency ICT Resources for political lobbying	Engaging directly or indirectly in partisan political activities by one holding non□political office
Copyright Infringement – Reproduction, duplication or transmission of copyrighted materials	Dishonesty
Criminal Use – Using the resources for criminal activities	Grave Misconduct
Stealing – stealing information resources both hardware or software or any part of the network resource	Grave Misconduct
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 Agency ICT Resources	Grave Misconduct
Password Disclosure – disclosure of user password protected account or making the account available to others without the permission of the E-mail System Administrator	Grave Misconduct
Unlawful Messages – use of electronic communication facilities (such as e-mail, talk, chat or systems with similar functions) to send fraudulent, harassing, obscene, threatening or other offensive messages	Simple Misconduct
Offensive Prohibited 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	Simple Misconduct
Prohibited Materials – using or encouraging the use of materials that includes instructions to gain unauthorized access (e.g. Hacker's Guide)	Simple Misconduct

Unauthorized reading of e-mail or private communications of other users, unless otherwise requested to do so by said user	Simple Misconduct
Misrepresentation in sending e-mail messages Falsification of official document	Simple Misconduct
Not cooperating with any investigative process in line with computer, network or system abuse	Violation of Reasonable Rules and Regulations
Disclosure of Agency Confidential Information – transmission of information without authority and/or proper security clearance	Disclosing or misusing confidential or classified information officially known to him by reason of his office and not available to the public, to further his private interests or give undue advantage to anyone or to prejudice the public interest
Access to lewd sites and/or materials – a user shall not view, transmit, retrieve, save or print any electronic file, image or text which may be deemed sexually explicit or pornographic	Violation of Reasonable Rules and Regulations

OFFENSE SANCTIONS

Engaging directly or indirectly in partisan political activities by one holding non□political office	1st Offense – Dismissal
Falsification of official document	1st Offense – Dismissal
Grave Misconduct	1st Offense – Dismissal
Dishonesty	1st Offense – Dismissal
Disclosing or misusing confidential or classified information officially known to him by reason of his office and not available to the public, to further his private interests or give undue advantage to anyone or to prejudice the public interest	1st Offense – Suspension for six (6) months and one (1) day to one (1) year 2nd Offense – Dismissal
Conduct Prejudicial to the Best Interest of the Service	1st Offense – Suspension for six (6) months and one (1) day to one (1) year 2nd Offense – Dismissal

Simple Misconduct	1st Offense – Suspension for one (1) month and one (1) day to six (6) months 2nd Offense – Dismissal
Violation of existing Civil Service law and rules of serious nature	1st Offense – Suspension for one (1) month and one (1) day to six (6) months 2nd Offense – Dismissal
Violation of Reasonable Office Rules and Regulations	1st Offense – Reprimand 2nd Offense – Suspension for one (1) to thirty (30) days 3rd Offense – Dismissal