DEPARTMENT OF THE NAVY
NAVY RECRUITING DISTRICT, PORTLAND
7028 N.E. 79TH COURT
PORTLAND, OREGON 97218-2813

NAVCRUITDISTPORTLANDINST 5230.1A
SYSAD
25 Mar 13

NAVCRUITDISTPORTLANDINST INSTRUCTION 5230.1A

Subj: OUTLOOK WEB ACCESS (OWA) TO NMCI

Ref: (a) NAVCYBERDEFOPSCOM NORFOLK VA(uc) P 072051Z DEC 06
(b) DON CIO WASHINGTON DC 161957Z OCT 02

Encl: (1) Request For Remote Access Form
(2) OWA User Responsibilities and Acknowledgement

1. Purpose. To promulgate instructions on authorizing Outlook Web Access(OWA) from non-Department of Defense(DoD) computers.

2. Background. As stated in references (a) and (b), OWA is to be provided only when necessary for mission accomplishment and OWA is not to be provided solely for convenience. The command must review all requests for OWA access and approve only those for which a bona fide requirement exists. Authorized Users must be knowledgeable of their responsibilities and the risks associated with the use of OWA access, and take appropriate action to mitigate those risks prior to being granted access to OWA. Middleware and Common Access Card (CAC) reader are required to authenticate Authorized Users.

3. Policy. When remote access is required by Navy Recruiting District Portland (NRD) military, civil service, or contract personnel, that individual is normally assigned a Navy/Marine Corps Intranet (NMCI) laptop which provides dial-up and broadband remote access service (BRAS). In some network configurations, OWA via BRAS is more efficient than using Outlook. If Outlook-based e-mail via the NMCI laptop does not provide sufficient remote access, at the convenience and discretion of the command, permission may be granted to access e-mail via OWA. When OWA access is deemed necessary from non-DoD computers, the command will provide the middleware and CAC reader for the user who completes the request for OWA described in this instruction.

4. Action

a. Department Heads are responsible for validating OWA access requirements using enclosure (1). The validation process includes coordination with Supply Department to purchase the appropriate number of CAC readers.

b. **Prospective OWA users will complete and forward the Request for Remote Access form, enclosure (1), through the Chain of command to their Department Head; complete the OWA training courses "NMCI Outlook Web Access (OWA)" "Securing non-DOD Computer for OWA," and complete the actions required by and sign the OWA User Responsibilities and Acknowledgement, enclosure (2).**

c. The NRD Portland Information Assurance Technician (IAT) will retain all approved requests (enclosure (1)) and their enclosures for one year after OWA access is no longer required or the individual no longer works for NRD Portland. IATs will provide annual refresher training to authorized OWA users.

d. The Commanding Officer shall be the approval authority for authorizing remote access to unclassified e-mail using personally owned and other non-DoD computers for personnel with a verifiable need.

e. The Information Assurance Technician will obtain sufficient CAC readers from the supply department, will control distribution of CAC readers to individuals who have been approved for OWA access, and will receive CAC readers from individuals prior to transfer or when they no longer require the use of the CAC reader.

f. Personnel for whom OWA is granted must comply with approved procedures and computer configuration requirements of enclosure (2).

R. M. CANDILORO

Distribution:
NAVCRUITDISTPORTLANDINST 5216.1U
Lists A, B, C, and D

NAVCRUITDISTPORTLANDINST 5230.1A
25 Mar 13

From: _____ (requestor)
To: Commanding Officer, Navy Recruiting District Portland
Via: Department Head (_____)

Subj: REQUEST FOR REMOTE ACCESS TO UNCLASSIFIED E-MAIL BY NON-DOD COMPUTER

Ref: (a) NAVCRUITDISTPORTLANDINST 5230.1A

Encl: (1) OWA User Responsibilities and Acknowledgement
(2) OWA Training Completion Certificate

1. I have read, understand and signed enclosure (1) and completed Outlook Web Access (OWA) and Securing non-DOD Computer for OWA training provided by Navy Marine Corps Intranet (NMCI) and have attached my certificate of completion as enclosure (2). In accordance with reference (a) I am requesting remote access capability to unclassified e-mail account:

_____@navy.mil

2. I require access for the following reason(s):

_____

_____

3. I have installed and maintain both the antivirus software and signatures current on the computer(s) I use to access OWA. I have installed and maintain a firewall on (or protecting) the computer(s) I use to access OWA.

_____
requestor signature

FIRST ENDORSEMENT on _____ ltr of _____
requestor date

_____
date

From: Department Head (____)
To: Commanding Officer, Navy Recruiting District Portland

Subj: REQUEST FOR REMOTE ACCESS TO UNCLASSIFIED E-MAIL BY NON-DOD COMPUTER

1. Forwarded recommending approval/disapproval (circle one) for access to OWA.

2. I have coordinated with the supply department to (add requestor to list of users authorized to borrow a CAC reader and middleware)/(purchase CAC reader for requestor until transfer or separation).

_____

- - - - - - - - - - - - - -

_____
date

From: Commanding Officer, Navy Recruiting District Portland
To: Information Assurance Technician (IAT)

1. Per reference (a), this OWA access is approved/disapproved.

_____
By direction

NAVCRUITDISTPORTLAND

OWA USER RESPONSIBILITIES AND ACKNOWLEDGEMENT

TO UNCLASSIFIED EMAIL

Name (Last, First, M.I.) (Please print clearly)	**Rank, Rate**	**Dept/Div/Code**

***PRIVACY ACT STATEMENT** **Account name** **Phone**

Disclosure of this information is voluntary. However, nondisclosure shall result in denial of remote IT system access. Authority to request this information is contained in 5 U.S.C. § 301 for the purpose of requesting information to ensure that all military, civilian, and contractor personnel who have signed this security briefing/user Acknowledgement form are correctly identified. Also 10 U.S.C. Part II and 14 U.S.C. Chapter 11 provide authority for the Command Information Assurance Technician (IAT) to use the above data to ensure proper security indoctrination of all assigned personnel.

I understand or have completed, as applicable: (initial each item)

___ That using Outlook Web Access (OWA) poses risks to the network, some of which are described in the OWA Web-based training I completed.

___ A demonstrated need, as certified by the Commanding Officer, is required for OWA use. Use of CAC-based PKI certificates is mandatory and must be installed on the non-DoD computer with high security enabled.

___ Use of personal firewall software, with port/protocol filtering features enabled, is required on the computer used to access OWA. Firewall settings are configured to "deny all" and allow by exceptions known applications. Government source software is available to support this requirement for all DoD employees and contractors as described at https://infosec.navy.mil.

__ Antivirus software and current virus signatures are installed and updated at least weekly on the computer used to access OWA. Managing the network health of the non-DoD computer is the responsibility of the user. Government source software and updated signatures are available to support this requirement for all DoD employees and contractors as described at https://infosec.navy.mil.

___ Software patches and security updates for operating system, applications, and web browser are maintained current.

___ No peer-to-peer file sharing programs (e.g. Kazaa, Skype, or Morpheus) shall be installed.

___ Password protection should be enabled on non-DoD computers to ensure family members or other unauthorized users do not inadvertently access OWA. Password-protected screen-lock will be set to activate within 15 minutes of inactivity.

___ Mail share programs are not allowed.

___ Only hardwired connections may be used. Ensure that no wireless or other LAN connection exists for the duration of the session. Any other existing connections must be disabled for the duration of the session. Except for the standard network interface device and directly connected printer, no peripherals should be connected while user is accessing OWA.

___ Users must delete all temporary internet files, close the browser and re-boot the non-DoD computer upon logging off OWA. Using Internet Explorer: Tools => "Internet Options" => General tab => "Delete files" Firefox: Tools => Clear Private Data.

___ Use of OWA to access a NMCI account requires the user to adhere to all NMCI rules and procedures.

___ As a government OWA user I agree to unlimited government monitoring with no expectation of privacy from government authorities of my OWA designated account, whether at home, on travel, or my fixed government account.

___ Violations of this policy may result in loss of access privileges and/or disciplinary action. In addition, military, government, or contractor personnel may be subject to criminal penalties if they knowingly, willfully, or negligently violate this policy.

___ Sensitive Information and Personally Identifiable Information (PII) of others will not be viewed or processed on non-DoD computers. In the event of this occurring, the file will be deleted before logging off and, where possible, overwritten (one overwrite is sufficient) using a Federally certified utility or utility from a major anti-virus vendor.

___ Prior to permanently leaving this command (e.g. transfer, retirement, separation, contract terminates), or if I no longer require OWA access, I agree to uninstall the middleware from my non-DoD computer and return the CAC reader to the appropriate person at my command.

___ OWA will not be accessed from public terminals such as libraries, colleges or airport/hotel business kiosks.

___ The following guidelines apply if classified information is found on the non-DoD computer (e.g. while using OWA):

- **Disable and unplug all network connections**
- **Do not transfer, copy, or forward any emails until the compromised classified information is fully sanitized or cleared as directed by member's command (IAT/Security Manager/CO) or other appropriate authority.**
- **Do not attempt to delete or move to the trash bin any compromised classified information without explicit instructions or authorization from member's command IAT or other appropriate authority.**
- **Report the names of anyone else that may have also received or come in contact with the compromised information.**
- **Do not allow any family members or friends to come in contact or view the compromised information.**
- **If required, your local IAT or Security Manager may need to conduct a non-disclosure briefing.**
- **All E-mail messages created using OWA, sent or retrieved over OWA from a Non-DoD computer system are the property of the U.S.**

Government. The U.S. Government reserves the right to access the contents of any messages processed over its facilities if it believes such access is necessary for security, as evidence of violation of existing instructions or policy or to maintain good order and discipline. And if warranted, removal of the member's privately owned hard drive, floppy or storage device medias as necessary to safeguard and protect U.S. classified information.

By my signature below, I certify that I have read and understand this policy and agree to adhere to the direction contained herein. This form will be retained by the NRD Portland Information Assurance Technician (IAT).

Signature: _____ Date: _____

System Serial Number(s) of Non-DoD computer(s): _____

Location: _____ Laptop: yes / no (circle)
(City/State)