

# **NOAA Unified Messaging Service Operational Procedures**

**NOAA Unified Messaging Service**

Enterprise Messaging Committee

**March 2012**

# Table of Contents

1. Purpose
2. Roles and Responsibilities
  - 2.1 Enterprise Messaging Committee (EMC)
  - 2.2 NOAA Messaging Operation Center (MOC)
  - 2.3 UMS Project Manager
  - 2.4 Account Administrators
3. Acceptable Use
  - 3.1 Abuse
  - 3.2 Privacy
  - 3.3 External Communications
  - 3.4 Sensitive or Confidential Information
4. Email Account
  - 4.1 Email Addresses
  - 4.2 Display Names
  - 4.3 Duplicate Names
  - 4.4 Authorized Access
  - 4.5 Employee Status Changes
5. Calendar Resources
  - 5.1 Calendar Resources
  - 5.2 Calendar Resource Account Request Process
  - 5.3 Calendar Resource Naming Conventions
  - 5.4 Calendar Resource Management
6. Account Functionality
  - 6.1 Mailbox Size Limits
  - 6.2 Email Client Use
  - 6.3 Calendar Client Use
  - 6.4 Message Size Limit
  - 6.5 Outgoing Message Limits
  - 6.6 Deleted Item Retention
  - 6.7 Forensics Investigations – Email Retrieval
7. Distribution Lists
  - 7.1 Distribution List Request Process
  - 7.2 Distribution List Naming Convention

8. Mobile Devices
  9. Instant Messaging
  10. Anti-Virus
  11. Support and Escalation
  12. Service Change Control
  13. Funding and Billing
- Appendix A: Email Best Practices
- Appendix B: Mobile Device Policies

## 1. Purpose

The purpose of this document is to define the recommendations made by the Enterprise Messaging Committee (EMC) regarding the administration and use of NOAA's Unified Messaging Service (UMS), the NOAA Enterprise Directory Service (NEDS), and the legacy NOAA Enterprise Messaging System (NEMS). This document is intended to ensure the proper use of NOAA's UMS infrastructure and to inform users of acceptable practices when working with these services.

NOAA reserves the right to amend this policy at EMC discretion. In case of amendments, users will be informed appropriately. The authority for this document is derived from NOAA Policy Directive M-3, NOAA Enterprise Messaging System Policy ([http://www.cio.noaa.gov/Policy\\_Programs/ciopol.html](http://www.cio.noaa.gov/Policy_Programs/ciopol.html)).

## 2. Roles and Responsibilities

### 2.1. Enterprise Messaging Committee (EMC)

The EMC was established to provide oversight for NOAA's UMS through its life-cycle. The EMC is comprised of one representative from each of the major Line and Staff Offices (NESDIS, NMFS, NOS, NWS, OAR, NMAO and HDQ) and the UMS Project Manager. The EMC is a standing board and is governed by a formal charter by the CIO Council. Developing guidelines and recommending policy is an assigned duty of the EMC. Refer to [http://www.cio.noaa.gov/pdfs/EMC\\_Terms\\_Of\\_Reference\\_1.pdf](http://www.cio.noaa.gov/pdfs/EMC_Terms_Of_Reference_1.pdf) for additional information.

### 2.2. NOAA Messaging Operation Center (MOC)

The NOAA Messaging Operations Center (MOC) is responsible for the administration of the NOAA Enterprise Directory Service (NEDS) and the centralized components of the legacy NEMS services until they are retired. Oversight for the MOC is provided by the EMC.

### 2.3. UMS Project Manager

The UMS Project Manager is responsible for the administration of UMS infrastructure and services through the UMS contract. The UMS Project Manager will sit on the EMC as the operational manager for the services provided.

### 2.4. Account Administrators

Local computer and network support administrators manage user and client software issues, and may escalate tickets for troubleshooting problems, through the processes designated by the service providers. User accounts are managed and maintained in the NOAA Enterprise Directory Service. All assignments of access rights for user email and calendar is done by the Account Administrators through the NEDS administrative interface (<https://ai.nems.noaa.gov>). The MOC and UMS services do not directly support end users and do not manage end user accounts.

## 3. Acceptable Use

### 3.1. Abuse

Electronic Messaging within NOAA is provided for business purposes only. NOAA does recognize that some personal mail will traverse NOAA's messaging network, however, such correspondence should be kept to a minimum. The solicitation and/or distribution of non-NOAA related materials, particularly matters of a personal nature or for personal gain, are strictly prohibited.

Misuse of Electronic Messaging is a serious problem and is considered the same as any misuse of government property, information, or equipment. Serious misuse may be considered "Gross Misconduct" and the appropriate action will be taken.

All NOAA employees (including federal, commissioned, associates and contractors) must understand that Electronic Messaging is subject to the same rules that govern the use of other means of communication. Electronic Messaging is not removed from the legal, ethical, and social considerations that make us responsible citizens.

NOAA employees must ensure they never use electronic messaging services that include, but are not limited to, the following types of email abuses:

- Represent themselves as another person.
- Transmit or store material that would be considered inappropriate, offensive or disrespectful to others.
- Harass other employees.
- Provide information about, or lists of, company employees to non-NOAA employees.
- Participate in activities that interfere with their job or the jobs of other employees.
- Interfere with the operation of NOAA's Unified Messaging Service.
- Violate any law or the rights of any person.
- Lobby, endorse, or promote affiliation with a particular political party or person.
- Originate or forward chain letters, spam, or malicious messages.
- Transmit or store threatening, obscene, or harassing messages.
- Generate messages for personal gain.

Employees should never knowingly generate messages that damage, disable, or disrupt electronic messaging services on NOAA's messaging infrastructure.

Employees are permitted to send some personal messages, but such messages should be minimized and kept as short as possible.

Please refer to the NOAA Rules of Behavior (<http://noaa.learnsecuritywith.us>)

## **3.2. Privacy**

The intent of this policy to assure employees that lawful personal use outside of work time on personal equipment will not be a basis for disciplinary action by NOAA. This policy also protects NOAA employees from the consequences of inadvertent misuse of government resources, including NOAA's Unified Messaging Service / Google Apps for Government (GAfG).

- 1) Personal information, personal browsing history or files outside of the browser on any personally owned device such as home desktop, tablet, laptop, phone, or other communications device that accesses Google Apps for Government will not be observed or changed in any way by NOAA or DOC.
- 2) Neither NOAA nor DOC will track or retain search information, browsing histories or files outside the browser from a personally owned computer or other communications device while it is not connected to a NOAA network, even if that information is inadvertently associated with a NOAA Google Apps for Government ID.
- 3) Using a personally owned computer or other communications device for personal activity while it is not connected to a NOAA network, even if simultaneously logged in to Google Apps for Government, shall not be the basis for any NOAA or DOC sanction or disciplinary action as long as the use does not violate any other applicable law or regulation.
- 4) Inadvertent observation of material or content that would otherwise be prohibited by this policy shall not be the sole basis for any NOAA or DOC sanction or disciplinary action for NOAA IT personnel (including network or administrative support staff) who are performing official duties while supporting NOAA users.
- 5) Using or installing Google Apps for Government will not reduce, forfeit, or otherwise limit anyone's right to use or store information on their personally owned computer, personally owned communications device or personally owned computer networks. However, all relevant legal requirements and existing NOAA and DOC IT policies governing user conduct and the use of Government IT resources (e.g., rules about sending emails, sharing files, sensitive data, posting to NOAA sites, etc.) will apply when using Google Apps for Government.

## **3.3. External Communications**

Under no circumstances should any electronic data be automatically and indiscriminately sent to a non-NOAA person, mailbox, or entity. Applications which disseminate information to non-NOAA employees must be tightly monitored and controlled. Discretion should be used when communicating with non-NOAA employees and should be limited to that which is necessary to conduct NOAA business. Mail client or transport rules that automatically forward mail to an external source are only permitted with written authorization approved by the accounts IT System Security Officer.

## **3.4. Sensitive or Confidential Information**

NOAA depends on NOAA employees to use good judgment in discussing and transmitting sensitive issues via email. Users should consider the impact of distributing sensitive

information. Users must not transmit Personally Identifiable Information (PII) over the email system without the appropriate encryption. The protection of PII is wholly the responsibility of the end user.

## 4. Email Account

All email account requests, creations, deletions, and/or modifications must go through the NOAA Account Administrators. Please see the sections below for proper naming conventions. This standardized process eliminates the possibility of unauthorized account creation and modification, as well as, the creation of unforeseen problems in the email operation infrastructure.

All email accounts should be managed through the NEMS Admin Interface (<https://ai.nems.noaa.gov>).

New email accounts will be created in the NOAA Enterprise Directory Service and from there synchronized to create the account in Google. No accounts will be created directly in Google. The account synchronization process is run every hour, so once an account is created it may take up to an hour to be active for the user to login and send or receive mail. New accounts must have google.nems.noaa.gov set as the mail host.

### 4.1. Email Addresses

User Email Addresses will follow a simple convention of:

[GivenName.SurName@NOAA.gov](#)

This is an email address that will be generated automatically for all NOAA employees per mandate. Only the user's legal name will be used when creating accounts. In the case of a legal employee name change (i.e. marriage) the employee will be given a secondary alias temporarily which will become the new primary. After thirty days the old primary will be removed.

In addition to user accounts the directory may be used for Functional Accounts. These accounts are those that need credential in the directory and may have a Google mailbox associated with them. Functional accounts follow a naming convention of:

[LineOffice.Organization.Function@NOAA.gov](#)

In cases where the function is enterprise-wide then the "NOAA" pre-fix instead of a "Line Office" or "Organization" may be used appropriately (e.g. [NOAA.AGO.Helpdesk@noaa.gov](#) or [NOAA.Webmaster@noaa.gov](#)).

### 4.2. Display Names

A display name is the format in which a user's name will appear in the Global Address List (GAL). The format of the GAL display name is:

**SurName, GivenName**

Functional Accounts are displayed in the GAL as follows:

**LineOffice Organization Function**

### 4.3. Duplicate Names

In an enterprise, such as NOAA'S UMS, the possibility of duplicate names will arise. Duplicate names can affect both account names and email addresses. Names are assigned on a first come first serve basis. The example below uses John Smith for an account creation. A conflict is sure to arise with such a generic name. A second John Smith will need to have a numeral, middle initial or full middle name to differentiate between users. Nothing will be done to the account or address for the original John Smith. Example:

***Original***

- [John.Smith@NOAA.gov](mailto:John.Smith@NOAA.gov)

### **Duplicate**

- [John.R.Smith@NOAA.gov](mailto:John.R.Smith@NOAA.gov) - Notice this has a middle initial added to the email address. This is an alternative to appending the 2 to the end of the user's name.
- [John.Smith2@NOAA.gov](mailto:John.Smith2@NOAA.gov) - John.Smith2 will be the logon name of user
- [John.Robert.Smith@NOAA.gov](mailto:John.Robert.Smith@NOAA.gov) - John.Robert.Smith will be the logon name of user
- [John.Robert.Smith2@NOAA.gov](mailto:John.Robert.Smith2@NOAA.gov) - John.Robert.Smith2 will be the logon name of user

## **4.4. Authorized Access**

Email Operations and Help Desk staffs do not have the authority to access an employee's mailbox. The UMS Project Manager may authorize access for e-discovery purposes with a written request from the user's supervisor or senior management.

## **4.5. Employee Status Changes**

**Termination:** The employee's directory account should be suspended within 24 hours of notification, unless directed otherwise by senior management. To suspend an account the user's mail administrator will do the following in the Administrative Interface (AI):

- Change the user account "inetuserstatus" attribute to "deleted"
- Remove the password for the account (blank passwords are not permitted to authenticate)

Once the account is suspended in the directory it will automatically be removed from Google in 30 days. During this time the mail administrator or the user's supervisor should make arrangements to preserve any data the user had that might be needed by the organization. This includes:

- Preserving any emails offline that are needed for official records or litigation holds
- Preserving any documents or sites the employee was the owner of by changing the ownership on these objects
- Taking ownership of any calendar entries the user had made that need to be continued
- Changing the ownership of any other Google resources that were assigned to the account

Mailbox data will be inaccessible in Google after 30 days. However, email data is still preserved in Google Message Discovery (GMD) for archive purposes. GMD archives this data for the life of the service contract with Google (see the UMS Project Manager for details).

**Leave of absence:** Nothing is to be done to the employee mailbox. There shall be no forwarding rules of any kind placed on the employee mailbox during the period of absence. In the event the mailbox fills up during this period Google will respond to new mail with a non-delivery response (NDR) stating the mailbox is full. The user may set up an out-of-office notification.

**Vacation:** Nothing is to be done to the employee mailbox. There shall be no forwarding rules of any kind placed on the employee mailbox during the period of absence. In the

event the mailbox fills up during this period Google will respond to new mail with an NDR stating the mailbox is full. The user may set up an out-of-office notification.

**Transfers:** The Account Administrator should change the “Line Office” attribute in the directory to reflect the new value (if the user is changing Line Offices). The Account Administrator should also set the “primary mail administrator” (PMA) attribute to that of the new office where the employee is moving so they may maintain the account. Note that changing the “Line Office” attribute may affect a users access to Google capabilities as these can vary by Line Office.

## 5. Calendar Resources

NOAA’s Unified Messaging Service will also allow for Calendar Resources. Calendar Resources will be managed centrally by the UMS Project Manager. Neither end user nor Account Administrators will have the ability to create calendar resources. Calendar resources must closely follow the naming convention so as to be easily searchable within Google. Google will automatically index and sort calendar resources by their name, so variations in the naming convention can hinder calendar resource usability.

### 5.1. Calendar Resources

A resource calendar is a calendar representing a physical asset, such as a conference room or shared equipment. The resource calendar is primarily used for scheduling purposes. Users can access and schedule conference rooms and/or shared equipment via the resource calendar.

The following two types of resource calendars are currently being supported:

- Conference Room – Scheduling of conference rooms or other types of locations (including media rooms, training rooms, shared spaces, etc)
- Equipment – Tracking and scheduling of government equipment (including vehicles, laptops, projectors, etc.)

### 5.2 Calendar Resource Account Request Process

Account Administrators may request the addition of a resource through the ticket escalation process to the UMS Project Manager. All calendar resources will be created centrally by the support team for UMS using the procedures below.

### 5.3 Calendar Resource Naming Conventions

Calendar Resources Email Addresses will follow one of two naming conventions based on the type of Calendar Resource.

#### Conference Rooms

*Building/Location – Function – Room Number/Other Identifier (cap #)*

*Building/Location* is the physical location, either a building name or a street number for the facility the resource is located in.

*Function* is the type of resource using the following convention:

- LgConf – Large size conference room
- MdConf – Medium size conference room
- SmConf – Small size conference room

TR – Training room  
Audi - Auditorium

If the function does not fit one of these categories other function descriptions may be used. They should be kept short though so as to be easily usable in the calendar interface.

*Room Number/Other Identifier (cap #)* is the room number for the room or location within the facility of the room. This is followed by the approximate capacity of the room in parentheses.

For example:

SSMC3 – LgConf – 9836 (cap 30)  
SSMC3 – LgConf – 12836 (cap 25)  
Suiteland – MdConf – 1110 (cap 15)  
DSRC – TR – 264 (cap 20)

## **Equipment**

*Line Office – Organization – Equipment Type*

For example:

NESDIS – NCDC – Pool Laptop 1  
NWS – PDX – Car Durango 00221  
OAR – HQ – Computer Projector  
NOAA – AGO – Slide Rule

Calendar Resources in Google also have a description field. The description field should include the following information about the resource:

*Manager Contact* – The name and a contact number for the resource manager.

*Resource Capabilities* – The capabilities of the resource should be described, like for example if there is a projector in the room, VTC equipment, telephone equipment, wired or wireless network access, etc.

*Scheduling Restrictions* – Any type of scheduling restrictions for the resource should be described especially for resources where approval is needed or physical access to the resource must be coordinated outside of the Calendar system.

## **5.4 Calendar Resource Management**

Calendar Resources will be managed centrally by the UMS service provider through the UMS Project Manager. Access to schedule calendar resources or restrict scheduling of resources may be configured within the capabilities of Google. The ability to control this access may be delegated to an Account Administrator limited by the functionality provided by Google.

## **6. Account Functionality**

### **6.1 Mailbox Size Limits**

Google mailboxes are limited to 25GB in size. If a mailbox goes over this limit then mail will no longer be received and the account will no longer be able to send. Mail sent to

the account will generate a non-delivery return (NDR) back to the sender. When the mailbox size is brought back below this threshold the account will again be able to send and receive mail.

## 6.2 Email Client Use

The Google service allows for access via IMAPS and HTTPS protocols. Email clients that use these protocols may be utilized by the end users. However, email clients must be deployed within the bounds of the NOAA Enterprise Architecture (EA) Technical Reference Model (TRM). In addition, any NOAA Line Office may set their own standards for supported email clients.

The UMS service contract supports only Thunderbird, Outlook, Entourage, and Mac Mail clients. It is recommended that Outlook users also utilize Google Apps Sync for Microsoft Outlook (GASMO) when using Outlook to provide integrated Google apps functionality for features like chat and calendar. Revisions to the client list are handled through the EMC's configuration change control process.

In addition to clients it is recommended the user access their email through the Google web interface. This interface is accessible on the internet (<http://www.google.com>) and provides functionality not available through other clients.

## 6.3 Calendar Client Use

The only supported access to the Google Calendar is through the web interface. No Calendar clients are supported or included in the NOAA EA TRM at this time.

## 6.4 Message Size Limit

Google limits the size of individual messages to 25MB. The 25MB limit includes the combined size of the message and the attachments. This means that you will not be able to send a 25MB attachment because the size of the message or the text contained within the email message is added to the total size; making the email larger than 25MB.

For larger attachments Google Docs may be used to share between NOAA accounts using the UMS. Google Docs policy and procedures are available on the NOAA CIO website (<http://cio.noaa.gov>).

## 6.5 Outgoing Message Limits

Google limits the number of messages a customer can send per day and the number of recipients they can address at one time. Google sets these limitations on all users in order to prevent anyone from becoming a repetitive "spammer". The latest limits on the number of messages can be found here:

<http://www.google.com/support/a/bin/answer.py?answer=166852>

Additionally, there is a limitation of 100 recipients when composing a message in Outlook, Thunderbird, MacMail, or Entourage (<https://mail.google.com/support/bin/answer.py?answer=22839>). It is recommended that user needing to send messages to wide distributions use email groups to do so.

## 6.6 Deleted Item Retention

Deleted emails are retained in the trash folder for 30 days. Items will automatically be removed from the trash folder after this time. Once an item has been removed from the trash it may be recovered by the account manager escalating a ticket to the UMS service provider.

Please note that only individual messages can be recovered this way through the GMD archive. Message folders, labels, and state (read, unread, etc) are not retained and cannot be restored.

The GMD archive retains messages up through the contract period. For additional information please see the UMS Project Manager for contract details.

## 6.7 Forensics Investigations – Email Retrieval

Email message retrieval or recovery from GMD is available for e-discovery purposes only through written request to the UMS service provider through the UMS Project Manager. There are no tape backups of data stored on Google and NOAA makes no local copies of this data.

## 7. Distribution Lists

Global distribution lists provide a lot of overlapping functionality with Google Groups. However, to insure that Google Groups can be properly mail-enabled they must be implemented with the following procedure:

- All distribution lists and Google Groups are to be created and maintained by Account Administrators only. Users will not have the ability to directly create lists or groups.
- All distribution lists and Google Groups must be created first in the NOAA Enterprise Directory Service LDAP directory. From there they will replicate over to Google with the synchronization process in place between the two directories.
- All distribution lists must follow the naming convention as described below.
- Distribution list membership should be maintained by the assigned group owner and group owners are recommended to review membership at least annually.

### 7.1 Distribution List Request Process

Account Administrators may create groups in the NOAA Enterprise Directory Service through the Administrative Interface (<https://ai.nems.noaa.gov>). These distribution lists should be approved using local processes determined by either the local office or the Line Office.

### 7.2 Distribution List Naming Convention

Distribution list must be compliant with the following naming convention:

*\_LineOffice Organization ListName*

The Distribution List naming convention will begin with an underscore character and the abbreviation for the Line Office (or NOAA in cases of enterprise level lists). Lists that do not follow the naming convention may be deleted without notice.

Distribution list must be compliant with the following email address convention:

*LineOffice.Organization.ListName@noaa.gov*

For example:

- \_NOAA Directory Admins ([noaa.directory.admins@noaa.gov](mailto:noaa.directory.admins@noaa.gov))
- \_OAR HQ NURP Employees ([oar.hq.nurp@noaa.gov](mailto:oar.hq.nurp@noaa.gov))
- \_NOS DAC SW ([nos.dac.sw@noaa.gov](mailto:nos.dac.sw@noaa.gov))

Distribution Lists will be accessible through Google as external mail contacts automatically, but will not be enabled as Google Groups. A Distribution List may be enabled as a Google Group with the approval of the UMS Project Manager. Account Administrators may submit a request to the UMS service provider to have a Distribution List enabled as a Google Group.

## 8. Mobile Devices

NOAA has a separate policy for the implementation and management of mobile devices. These devices must still abide by all of the policy for email access found here. The management of mobile devices and configuration changes to services for mobile devices are within the scope of the EMC. See Appendix B for the policy.

## 9. Instant Messaging

Google Chat provides instant messaging service for all NOAA users that have a Google account. This service is open to allow text-based instant messaging, voice communications, or video chat sessions for NOAA user with any other Google user. This includes allowing messaging with users outside of the noaa.gov domain.

Per the decision of NOAA General Counsel all instant messaging sessions will be considered “off the record” and will not be recorded in anyway. Much like a phone call they are intended to be informal exchanges of information. All official records should be documented appropriately through other means.

## 10. Anti-Virus

The UMS service provided by Google uses Postini anti-virus scanning for all inbound and outbound email. This scanning service will automatically adjust to threats and filter out malicious messages or messages with malicious attachments.

In addition, custom filters can be put into place to block malicious messages. Custom filters can be requested by Account Administrators from the UMS service provider through the UMS Project Manager.

## 11. Support and Escalation

The UMS service provider is responsible for tier three level support through the UMS Project Manager. All end user support should be routed through the appropriate helpdesks for tier one support and then from there to Account Administrators for tier two. If the end user requires additional support then Account Administrators may escalate to the UMS service provider using their online ticketing system ([https://docs.google.com/a/noaa.gov/spreadsheet/viewform?hl=en\\_US&formkey=dHlzXzU3V2U0MzhpVm5vZk1rMG5TMIE6MQ#gid=0](https://docs.google.com/a/noaa.gov/spreadsheet/viewform?hl=en_US&formkey=dHlzXzU3V2U0MzhpVm5vZk1rMG5TMIE6MQ#gid=0)).

Please see the UMS Support website (<https://sites.google.com/a/noaa.gov/noaa-ums/get-help/support-desk>) for more information including a flow chart of the escalation process:

[https://docs.google.com/a/noaa.gov/viewer?a=v&pid=explorer&chrome=true&srcid=0B7VdJYuMnxEeOGRmNjY0N2MtNmM5NS00NGY3LTg5YzItN2ZIMTNkNzQwZDA5&hl=en\\_US](https://docs.google.com/a/noaa.gov/viewer?a=v&pid=explorer&chrome=true&srcid=0B7VdJYuMnxEeOGRmNjY0N2MtNmM5NS00NGY3LTg5YzItN2ZIMTNkNzQwZDA5&hl=en_US)

Support requests for anti-spam service, directory service issue and e-discovery requests should be escalated to [moc@noaa.gov](mailto:moc@noaa.gov) by Account Administrators.

## 12. Service Change Control

Configuration management for the UMS service is provided by the Enterprise Messaging Committee (EMC). All configuration change requests for Google services should be submitted to the EMC for evaluation and approval.

Please note that change requests may also need to be routed through another committee or working group depending on the area of Google services that they deal with (for example, change requests for Google Sites and Google Docs must receive approval by the NOAA Web Committee prior to consideration at the EMC).

Change requests are submitted to the EMC through email to the group of voting members ([emc@noaa.gov](mailto:emc@noaa.gov)). The EMC will then schedule an information briefing to the group and a decision briefing. If appropriate both information briefing and/or decision briefing may be done virtually over email at the discretion of the EMC Chair.

The EMC is a consensus group so unanimous approval is always preferred. However the EMC decision making process may be found in the committee's Terms of Reference ([http://cio.noaa.gov/IT\\_Groups/NOAA\\_Enterprise\\_Messaging\\_Committee\\_TORv2.pdf](http://cio.noaa.gov/IT_Groups/NOAA_Enterprise_Messaging_Committee_TORv2.pdf)). If consensus is not reached at the EMC, then it is suggested to elevate the configuration change request to the NOAA CIO Council.

## 13. Funding and Billing

The services covered under the NOAA Unified Messaging Policy are funded through the NOAA Direct Bill process. This process is set by the NOAA CFO Council. Each year's Direct Bill submissions will be reviewed and approved by the EMC. Current submissions are as follows:

**NOAA Enterprise Directory Service (NEDS)** – This direct bill covers the cost of running the LDAP directory service and the e-discovery component of the legacy email system. It is distributed among the Line Offices based on the total number of accounts they have in the LDAP directory.

**Unified Messaging Service (UMS)** – This direct bill covers the contract that supports the cloud email service with Google. This includes email, calendar, and collaboration services (such as chat, docs, and sites). It is distributed among the Line Offices based on the number of accounts they have in the Google directory. Note that not all accounts in the LDAP directory are in the Google directory. Google charges licensing on a per seat basis.

**Blackberry Enterprise Services (BES)** – This direct bill covers the cost of running the Blackberry Enterprise Services through the UMS support contract. It is distributed among the Line Offices based on the number of Blackberry devices activated on the BES servers.

## Appendix A: Email Best Practices

The following practices are common use for email. They are not required but are useful in better communication with other people using electronic messaging.

1. Emails should be well-written and use concise and descriptive subjects.
2. Delete any email messages that you do not need and are not required to maintain. Regularly archive your older messages.
3. Target communications. Messages should only be sent to those people who need to receive the information.
4. When replying to a message, check the message header for large distribution lists. Also do not retain unnecessary attachments.
5. Do not send unnecessary attachments. Large attachments should be zipped before sending to reduce the size.
6. Be careful when opening attachments or clicking on links as they might contain viruses or other malicious software.
7. Do not open email from unknown people.
8. Exercise good judgment in composing emails.
9. The following are some of the best practices for using the Google Web Interface in public locations:
  - a. Always close all the browsers when you are done using the web interface.
  - b. Do not open attachments on a non-trusted machine as temp files are sometimes left behind on the computer.
  - c. Don't leave the browser up when you step away, always logoff or lock the console if the option is available.
  - d. Pay attention to your surroundings when logging on ensuring that no one is watching you type in your password or other sensitive information.
10. Out-Of-Office notifications are available but use caution when enabling. Always use generic information when configuring your out-of-office agent.
  - a. **Good:** I have received your email. Unfortunately, I will be unavailable until 12/6/04. I will only be checking email or voicemail periodically during this period. In the case of an emergency, please contact Jodi Watley at 202-555-1212.
  - b. **Bad:** I will be out of town the week of 12/15/04 in a Project Management training class in Hawaii. In case of emergency, please contact Jodi Watley 202-555-1212.

Please note: Messages that are sent to all users in the organization are usually sent from members of NOAA leadership. If you feel that a message needs to be sent to the entire organization contact your local supervisor and they will determine the business need. Before asking management for approval, think about the following questions:

- Is the message Business related?
- Do you think management would approve sending this message to the entire organization?

If you know the answer to either of these questions is "NO", then the message should not be sent. Please DO NOT send messages to all users in the Global Address list without proper authorization.

When sending email messages and selecting recipients from the Global Address Book please verify that you have selected the correct recipients before clicking on the "send" button.

Also, remember to NOT select "Reply to All" when replying to messages that are sent to all users or to a large distribution groups. Please reply only to the originator of the email message.

# Appendix B: Mobile Device Policies

February 3, 2012  
Version 1.0

## NOAA Mobile Device Security Policy

### Introduction

Mobile computing devices, smart phones and tablet computers are important tools for the organization and their use is supported to achieve business goals. However, mobile devices also represent a significant risk to sensitive data and systems if appropriate controls are not applied.

NOAA and its component Line Offices have a requirement to protect its information assets in order to safeguard sensitive data including Personally and Business Identifiable Information, and other sensitive data. This document outlines a set of practices and requirements for the use of mobile devices.

### Scope

1. This policy applies to all mobile devices that have access to Government networks, data and systems. This includes smart phones and tablet computers except as noted below.
  - a. This policy does not apply to laptops encrypted, maintained and used in accordance with applicable NOAA policy and requirements
  - b. Devices that access government data exclusively through an official web portal and do not otherwise store or retain government data on the device.
2. Exemptions from this policy may be granted by the NOAA CIO or designee, on a case by case basis, after:
  - a. Demonstration of sufficient business need and;
  - b. Completion of a risk assessment by security management.

### Policy

Effective January 1, 2012:

1. Unless otherwise specifically stated in this policy, all Department of Commerce and NOAA IT security policies apply to mobile devices used to access NOAA systems.
2. Line Offices may require and enforce additional enhanced security controls.
3. Devices that connect to NOAA systems, except as specified as excluded in the Scope Section of this document, must be managed by a NOAA and / or Line Office mobile device management system. The management system may do or enforce the following:
  - a. Devices covered by this policy may not be used to access or store classified data.
  - b. All Government data on devices that connect to NOAA systems must be encrypted to a level approved by the NOAA CIO. This will be at least AES 256 encryption.
  - c. Devices that connect to NOAA systems must be configured with a password that complies with NOAA password policy.



UNITED STATES DEPARTMENT OF COMMERCE  
National Oceanic and Atmospheric Administration  
OFFICE OF THE CHIEF INFORMATION OFFICER  
High Performance Computing and Communications

FEB 03 2012

MEMORANDUM FOR: Assistant Administrators  
Deputy Assistant Administrators  
Staff Office Directors  
Line Office Chief Information Officers

FROM: Joseph F. Klimavicz   
NOAA Chief Information Officer and Director for High  
Performance Computing and Communications

SUBJECT: NOAA Mobile Device Policy

Mobile computing devices, smart phones and tablet computers are important tools and we support their use to achieve our business goals. However, mobile devices can also represent a significant risk to sensitive data if appropriate controls are not applied. NOAA chartered a team from across the line and staff offices to create a workable solution that allows for the use of modern mobile technology. Attached you will find the NOAA Mobile Device Policy and the NOAA Mobile Device Rules of Behavior. Implementation of the NOAA Mobile Use Policy will be consistent with NOAA's collective bargaining agreements and the Federal Service Labor-Management Relations Statute.

Managing mobile devices from the Unified Messaging Services (UMS) is a new capability for NOAA, and it is anticipated that the solution will be implemented in phases. Initially this implementation authorizes access to:

1. UMS applications including
  1. mail
  2. calendar
  3. contacts
  4. NOAA Google Docs
2. Government data through an official web portal.

NOAA will initially support only the following government furnished devices:

1. iPhone versions 4 and above with iOS 5 and above
2. iPad 2 and above with iOS 5 and above
3. Conventional cellular phones
4. Blackberry devices (support expected through May 2012)

The [UMS Home Page](#) will be updated with links to the attached policy, rules of behavior, as well as step by step procedures for connecting your approved device to the UMS. Changes to the list of authorized devices and or systems which may be accessed will be communicated by the NOAA CIO.



## NOAA Rules of Behavior for Mobile Devices

The purpose of this document is to outline the conditions NOAA requires to allow mobile devices to connect with NOAA systems including email. By signing this agreement the user agrees to abide by the NOAA IT Rules of Behavior, all other Department of Commerce, NOAA and Line Office IT Security Policies. In addition, the following will apply to any Mobile Devices configured to access NOAA systems including email. Specifically:

- NOAA and /or Line Office will install an IT Security Profile on all devices that connect to NOAA systems. The configuration may make some applications unusable. NOAA and / or Line Offices are not responsible for the cost or support of such applications.
- The user understands and agrees that all data on the device may be accessed and reviewed pursuant to government investigations and / or litigation. The user further understands that they may be without access to the device as a result of the review. NOAA and / or Line Office are not responsible for any cost for loss of use as a result of a review.
- Any device found to have attempted to change NOAA or Line Office installed security controls will be immediately wiped and removed from access to NOAA systems.
- NOAA and / or Line Office will not be responsible for costs or support associated with non-work related applications.
- Except for UMS data (email, calendar, contacts, and NOAA Google Documents) configured and managed by the processes published by NOAA, no government data may be stored on any device or location unless such storage is specifically authorized in the system security plan.
- Mobile devices may not be physically connected to NOAA systems or computers. This includes the use of USB chargers connected to a NOAA computer.
- NOAA and / or Line Office reserves the right to remote wipe devices at anytime with or without notice to the user.
- NOAA and / or Line Office may install security and management related software on mobile devices.
- NOAA and / or Line Office will not be liable for any loss of data or applications resulting from a remote wipe.
- Prior to taking the mobile device outside of the United States, for either business or personal travel, the user must notify the Line Office IT Security Officer or individual designated by the Line Office:
  - Dates of travel
  - Countries of travel including stopovers and layovers
  - Identify any sensitive data that will be on the mobile device during travel
  - Comply with organizationally defined practices including maintaining possession of the device at all times, disabling WiFi and Bluetooth services, and such other controls as the Department of Commerce Office of Security (OSY), NOAA, or Line Office may impose