PA DEPARTMENT OF PUBLIC WELFARE

SeGOV User Guide

Https Browser Users

Version 1.1

B A Wadlinger

3/16/2011

The document is a user guide for SeGOV users. It demonstrates the one-time administrative tasks required by security and also provides notes in use of the MoveIT Browser.

Contents

SeGOV – User Guide – Https Browser

This document represents a guide to the functionality available to the SeGOV Https Browser Users. Please refer to this document when navigating thru the browser screens. Use of SeGOV meets requirements set forth in OA Information Technology Bulletin (ITB SEC031- Encryption Standards for Data in Transit). This document can be accessed at

http://www.portal.state.pa.us/portal/server.pt/gateway/PTARGS_0_2_785_416_0_43/http%3B/pubcontent.state.pa.us/publishedcontent/publish/global/files/itbs/security_itbs/sec031/itb_sec031.doc.

SeGOV URL

PRODUCTION Login URL – https://missl.dpw.state.pa.us

TEST Login URL – https://missl-s.dpw.state.pa.us (Use only if Authorized)

SeGOV Users

SeGOV users are a member of one of the following domains
- Managed
- CWOPA

Two SeGov users are permitted per entity – Primary and Backup.

Each user is required to complete the required confidentiality agreements (i.e. User Agreement). This document will be accepted and registered in the database when the user creates HINT questions. Failure to accept this document may result in denial of access to SeGOV.

UserNames and Passwords **MAY NOT** be shared. Every user must have a unique UserName and Password. Two Users are permitted per Entity. Generic Accounts are no longer supported. If the information displayed is NOT correct, please contact your DPW Program Office coordinator to review and update the user information. You may need to obtain a new username if previous username is no longer valid (Generic Accounts are no longer supported). This means that as personnel changes are made, the old user will need to be deleted, and new user must be registered. User Registration forms are available thru the DPW Program Office coordinator. Please allow two weeks for this process. It is understood that there will be emergencies, but because of approvals required, same day service cannot be expected.

Invalid usernames will need to be disabled in DPW security system. Please provide following to DPW program office coordinator when a user no longer requires access to SeGOV:

Name of Individual
SeGov UserID Name (i.e. starts with "b-")
Business Entity Name
IP Address – if known or appropriate

To meet Commonwealth security standards, all users must be registered in Unified Security (USEC) and all IP addresses must be registered in Commonwealth Office of Administration (OA) firewall.

Users will have access to folders for upload/download of files as defined by the application requirements.
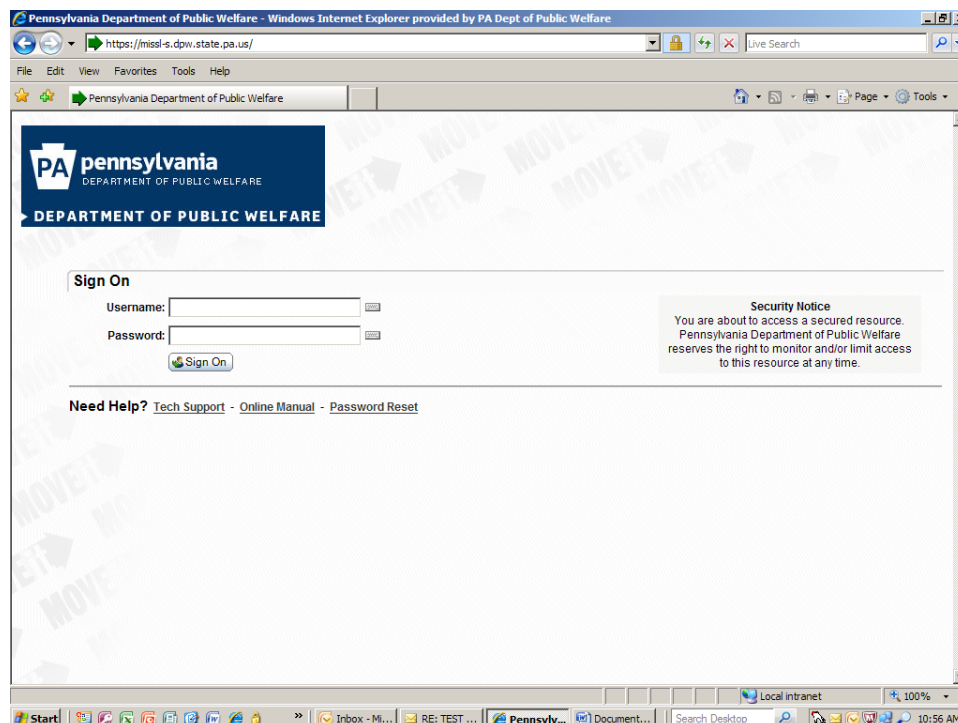
The DPW program office coordinator is the user interface to adding/removing users within SeGOV.

Getting Started

In order to utilize the Password Reset functionality, the DPW User Agreement and Self Service Password Hint Q/A Process must be completed.

Since this is a one-time process, there is no need to revisit this page once completed.

From the User Internet home page or favorite, open the SeGov URL: https://missl.dpw.state.pa.us

Select **Password Reset** from the "Sign On" screen above.

At the **Keystone Key** page (above), enter SeGov **Username** and **Password.**

Click **Login**

DPW USER AGREEMENT

The Reset Password functionality verifies that the User Agreement is on file with Active Directory (AD) maintained by the DPW Unified Security team (USEC). The user may have previously completed a physical form, However, to set the flag properly in AD, the user needs to "**Accept**" the DPW User Agreement at this time. Failure to accept the User Agreement will cause delays in use of the SeGOV application.

Please read the Management Directive (205.34). A copy of this document is supplied in Appendix 1 of this document.

Click "**I have read, fully understand and agree to the Management Directive MD 205.34**" on the screen below.

Click **Next**

User will receive **Task Completed** Message

Hint Questions

In order to utilize the Password Reset functionality, the Self Service Password Hint Q/A Process **must be completed.**

Since this is a **one-time process** there is no need to revisit this page once completed.

The next screen will bring the user to the **PW Update Hint Questions** page.

This must be completed for each SeGov user.

Passwords must be changed from this page when questions are created.

User Name - will be displayed

User First Name - will be Displayed

User Last Name - will be Displayed

Enter New Password – See Password rules to the right of the field

Confirm New Password

Enter Email Address *(it is very important that the user confirms this is the email address for their SeGov UserID – changes must be submitted through the Program Office Contact)*

Re-enter Email Address to Confirm (or review again that that the email address is correct)

Create Answers to three security Questions – Select Security Question from each of three drop-down lists. **Enter Answer –** this answer is unique to the user and should never be shared.

When used in change password, user must enter answer exactly as created here (If user enters that they grew up on Market Street; then Market Street is the correct answer to the HINT question).

Select Security Question 1

Enter Answer -recommend one-word answers all in small letters

Select Security Question 2

Enter Answer - recommend one-word answers all in small letters

Select Security Question 3

Enter Answer - recommend one-word answers all in small letters

Enter Primary Phone Number for user (must have all 10 digits)

Select **SUBMIT**

User may receive a message, "**Task has been submitted. Please wait…**"
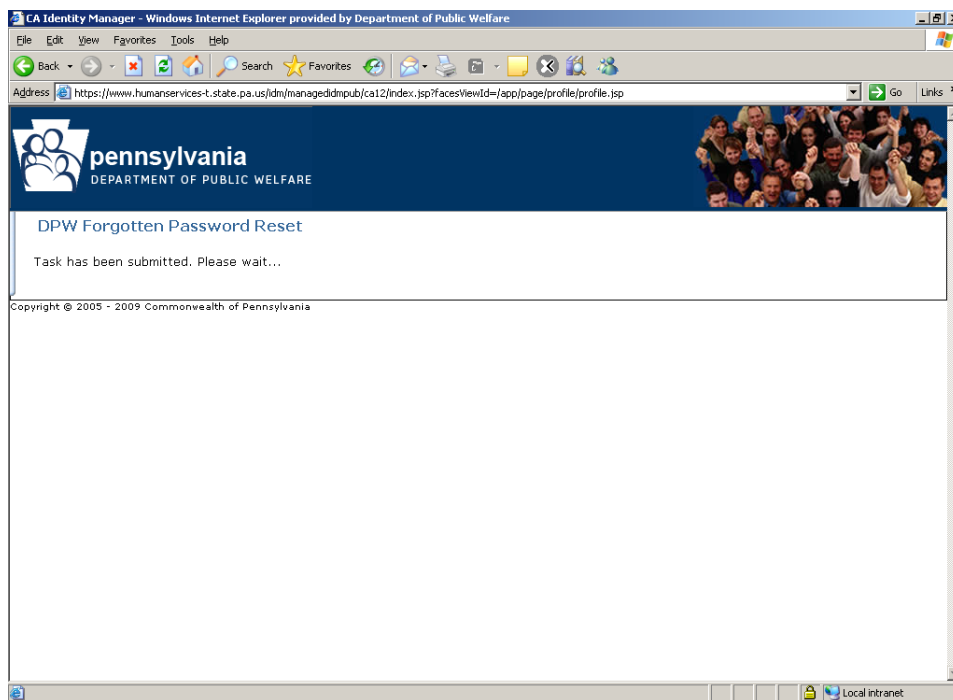
At this point user should receive a "**Task Completed**" message like the screen below. Password has now been changed.
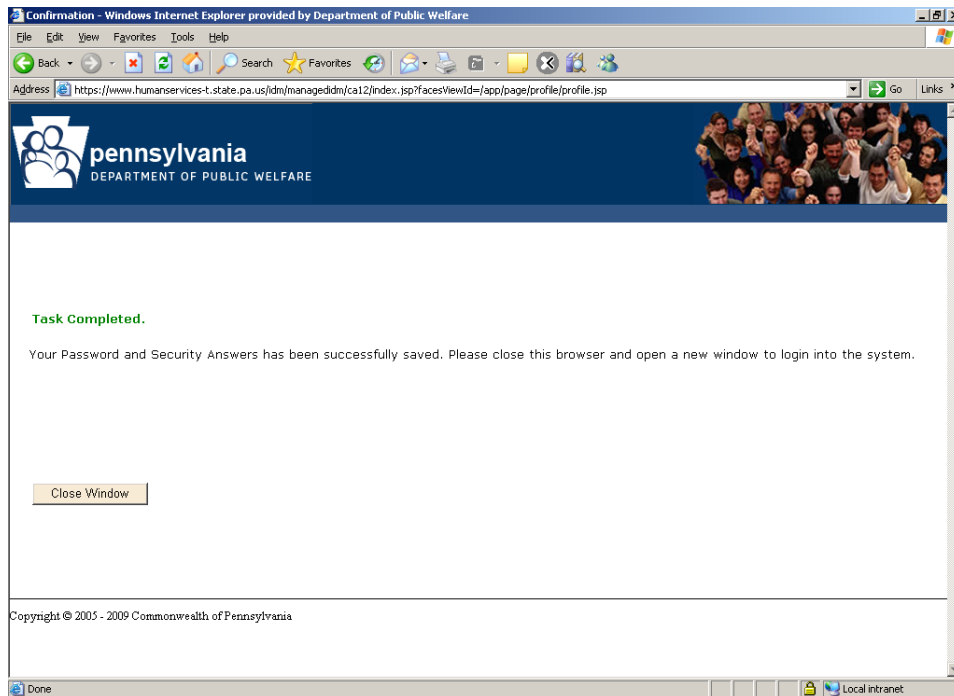
Click "**Close Window**"

User Hint Questions have been established.

Exit **ALL** Internet Browser sessions.

Click the SeGov URL to continue with the following configurations and procedures.

Forgot UserID?

Users are able to receive an email advising them of their forgotten UserID. *It is very important that the user information request match exactly to information on file in Active Directory.* This includes First Name, Last Name, and email address. If the user information has changed, user must submit the new information to their Program Office Coordinator for submission to USEC for change. Please submit the following information:

Business Entity Name
User Full Name (as was listed in Active Directory)
Domain: Managed PROD
SeGov UserID (starts with "b-)
Old email address
New email address
Phone Number

From the User's Internet Explorer (or other Internet browser) **Home** page or favorite, open the following SeGov URL: https://missl.dpw.state.pa.us
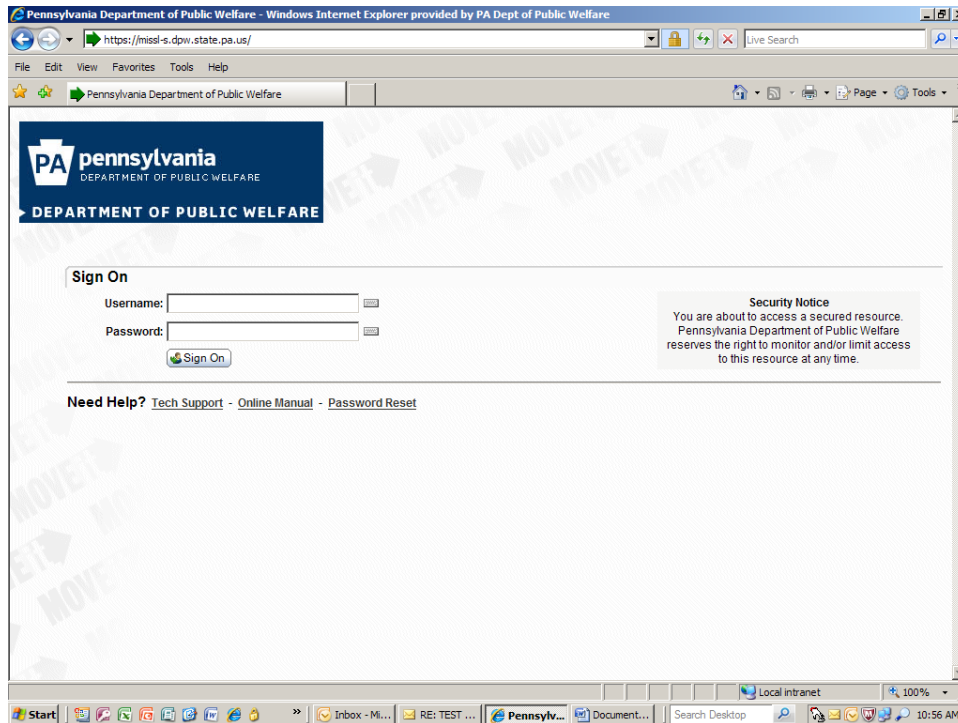
Select **Password Reset** from SeGov URL "**Sign On**" screen above.
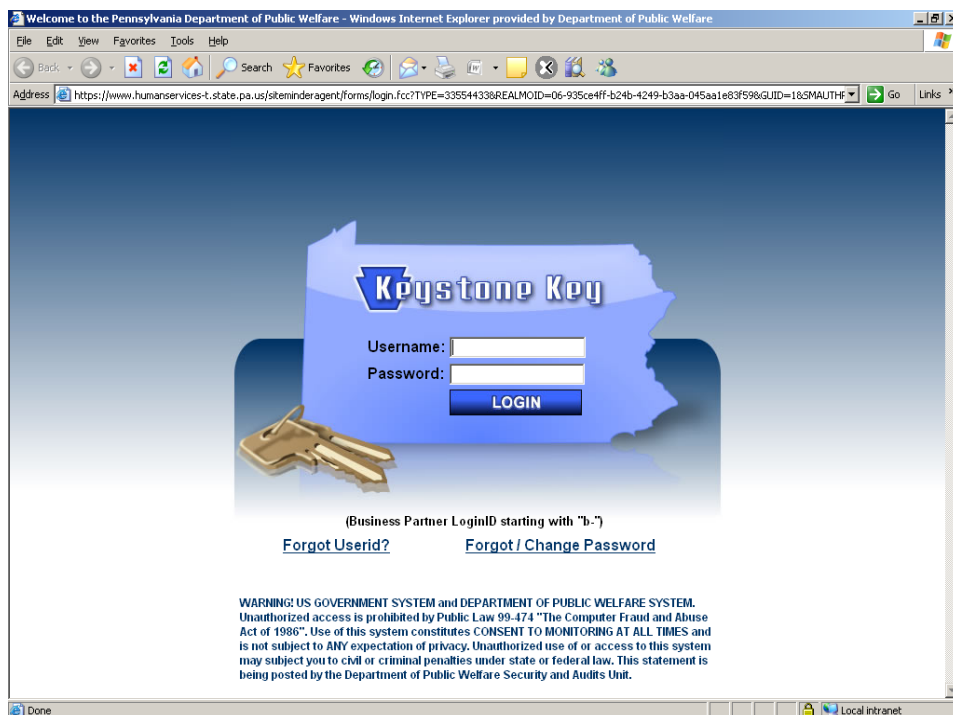
Select **"Forgot Userid?"** from the **Keystone Key** login screen (do **NOT** enter UserID or password).

Complete the information requested. This must match information as stored in Active Directory when the user registered for access to the Managed Domain.

Click **OK**

User will see a screen "**Confirmation: Task Completed**" as seen below:

Click "**Close Window**" in the screen above.

Exit **ALL** Internet Browser sessions.

User will receive an email like the one below:
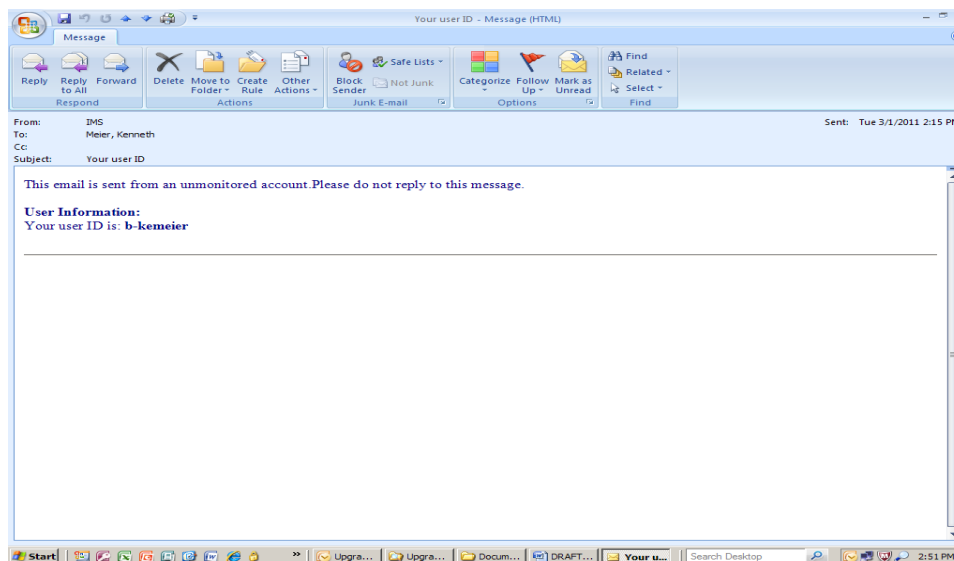
User is now able to reopen the SeGov URL and login with SeGov UserID and password.

Password Reset

All passwords expire and must be reset every 60 days. At this time there is no provision to notify the user in advance of this occurrence. The user must currently use a tickler system and change the password prior to 60 day expiration.

Failure to reset the password within 60-days will result in a disruption in connectivity to SeGov. User will not be able to access the SeGov site if their password has expired.

It is expected that **ALL** users will accept the 205.34 agreement and create HINT questions with answers. *If HINT questions have been created, the user will be able change the password even if it has expired.* If user receives error "Not enough information to complete HINT questions", the user has NOT completed the 205.34 agreement and created HINT questions.

If user has NOT created HINT questions, user will NOT be allowed to reset their password. Please contact OIS Account Administration at 1-800-281-5340 and then press #3. After the user supplies the SeGov UserID name, ask the service desk to reset the password. Please make sure that new password is clearly understood. Please wait ten minutes before attempting to use the new password.

 From the User's Internet Explorer (or other Internet browser) **Home** page or favorite, open the following SeGov URL: https://missl.dpw.state.pa.us.

Select **Password Reset** from the **Sign On** screen below (but do **NOT** enter your Username/password):
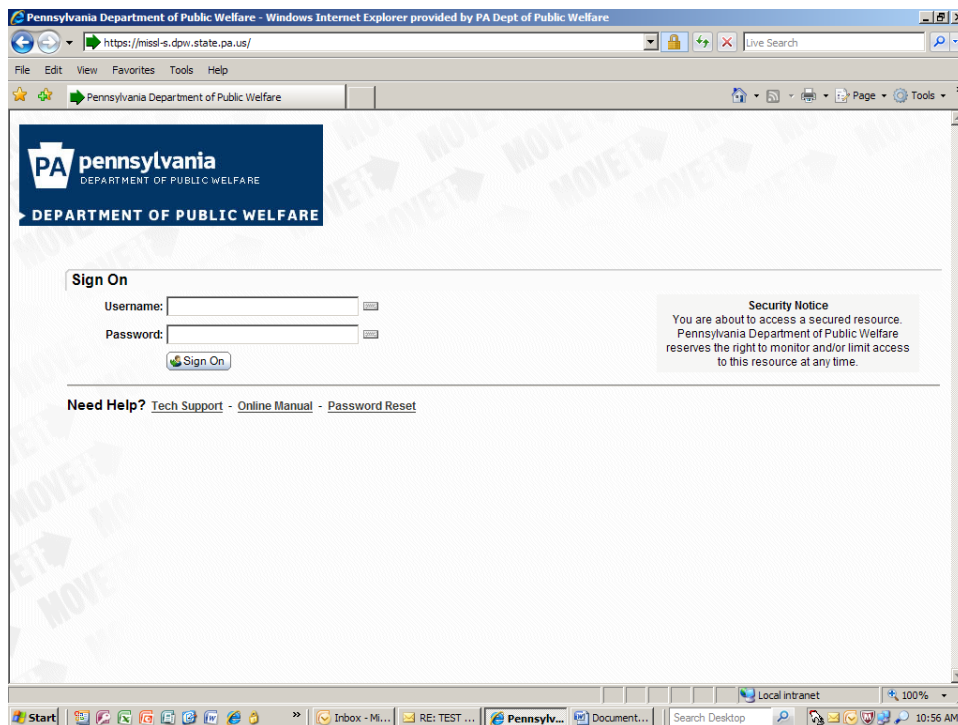
Click on **Forgot/Change Password** from the **Keystone Key** screen below:

Enter your UserID on the screen below.

Click **OK** on the screen above.

User information will be displayed on screen above. If this is **NOT** correct, please contact OIS Account Administration at 1-800-281-5340 and press #3 to get the information resolved.

User must answer two Hint Questions and then click **OK.**

Upon successful answers to two Hint Questions, user will be allowed to change their SeGov password.

Please follow the **Password Policy Requirements** as defined to the right of the password fields on the screen.

Click **Submit** on the screen above. The next screen will be the "**Task has been submitted. Please wait**" below:
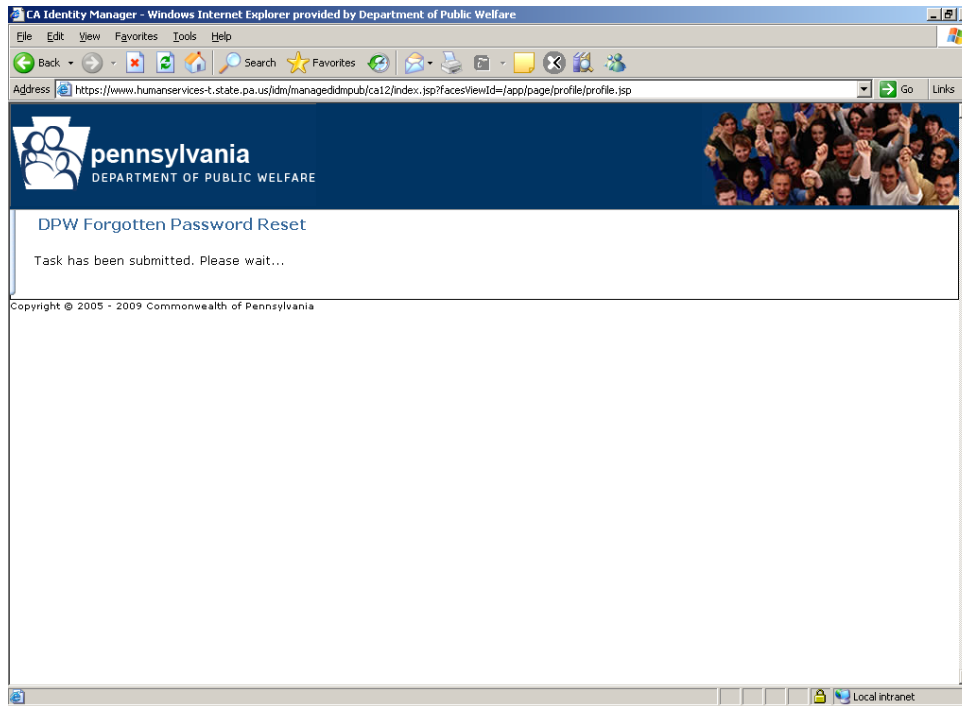
User may receive an error message that the password cannot be reset. User must re-enter password information according to rules at right of the password fields, and then click **Submit** again.

If the password was reset successfully, user will receive the "**Task Completed**" screen below:
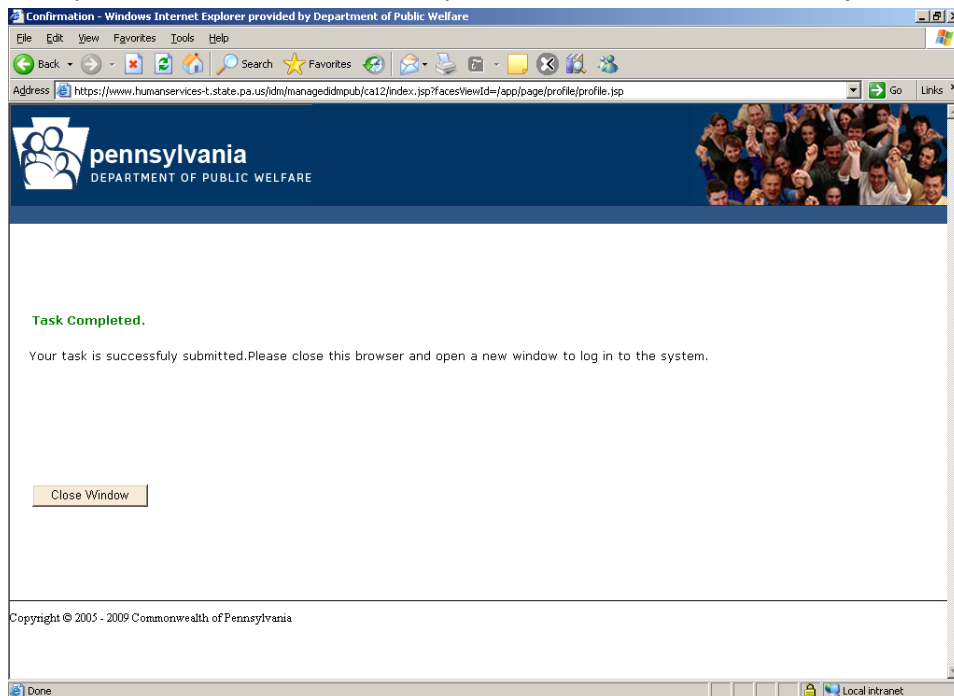
Click "Close Window" on the screen above.

Close **ALL** Internet Browser sessions.

OnLine Manual

This **Online Manual** link (in the screen shot below) provides an overview and general instructions from Software Provider. This is for reference only and does not fully support DPW use of this product.
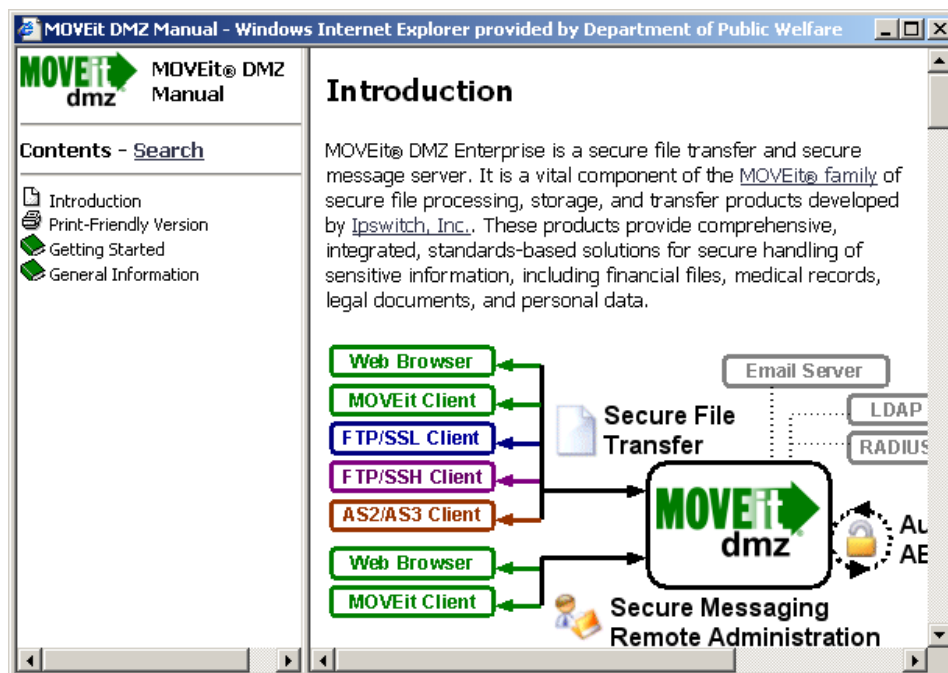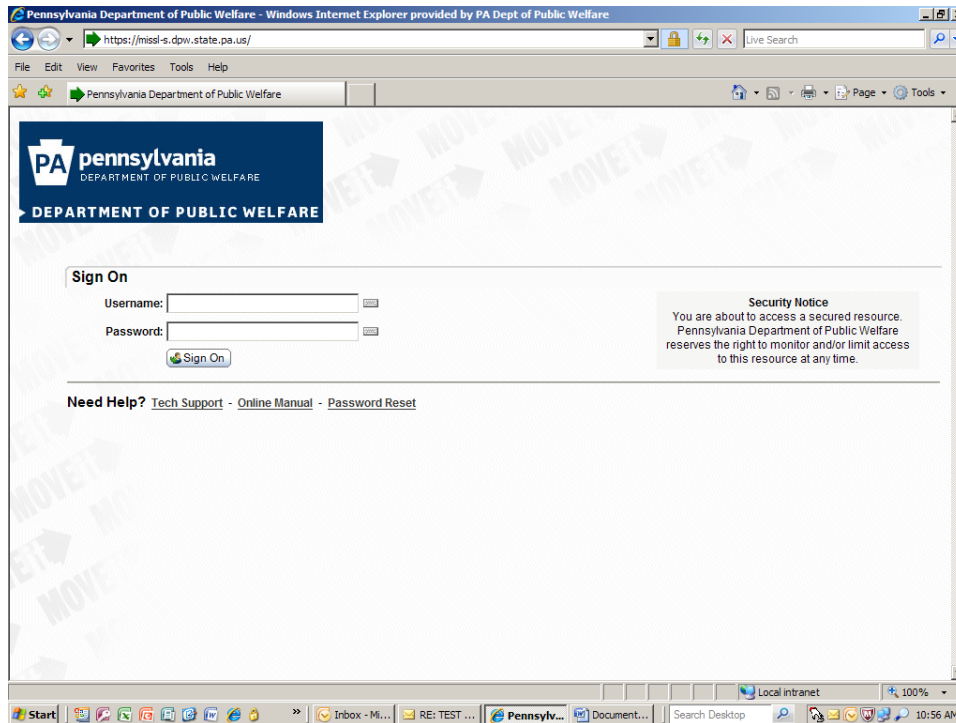
Using the SeGOV system

From the User's Internet Explorer (or other Internet browser) **Home** page or favorite, open the following SeGov URL: https://missl.dpw.state.pa.us

Sign-On with valid SeGov UserID (i.e. Username) and valid Password
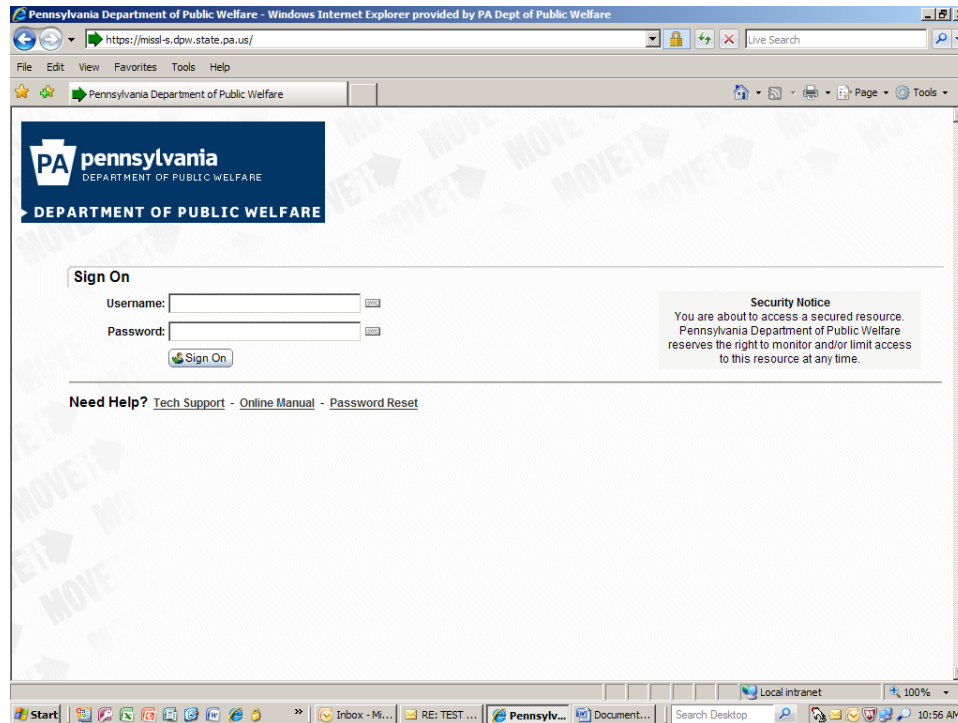
Troubleshooting

If user receives "**Page Cannot be Displayed"** error please review the following items:

- Validate that the SeGov URL is correct: https://missl.dpw.state.pa.us
- Make sure that you type in the SeGov URL above into the Internet Explorer address field (or in the Internet browser address filed of the browser that you use). Then click the green "**Go**" button.
- If using a favorite or desktop icon – Does URL match SeGOV URL.
- Validate that the IP address used to access the Internet is registered in the Commonwealth Internet Firewall. Contact your local user Information Technology (IT), Management Information System (MIS), or Internet Service Provider to answer any questions regarding IP addresses. If the IP address has changed, submit a request to update the IP address to the Program Office Coordinator. User will experience access failure until correct IP is registered.
  - The IP addresses must be routable, external, and static.
  - The IP addresses **can't** fall in the following ranges of IP addresses:

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

- o The IP address that SeGov needs is the IP address that the Commonwealth Internet Firewall will see when the SeGov UserID accesses the SeGov website.
- o A maximum of four IP addresses for each SeGov Business Entity that can be registered (i.e. some organizations have fail-over or backup servers to handle the work load).
- If user still cannot access SeGOV, contact the Program Office coordinator.

If user receives "**Invalid username/password or not allowed to sign on from this location":**

- Validate the SeGov UserID (i.e. "UserName") is correct
- Validate that the Password is correct
- Has the Password expired? The password expires after 60 days. The user will be locked out after five unsuccessful attempts to log in. (Go to Reset Password section)

Successful Log In to the SeGOV website:

User will be placed in their designated SeGov "**Home**" page, similar to the "**Home**" page below:
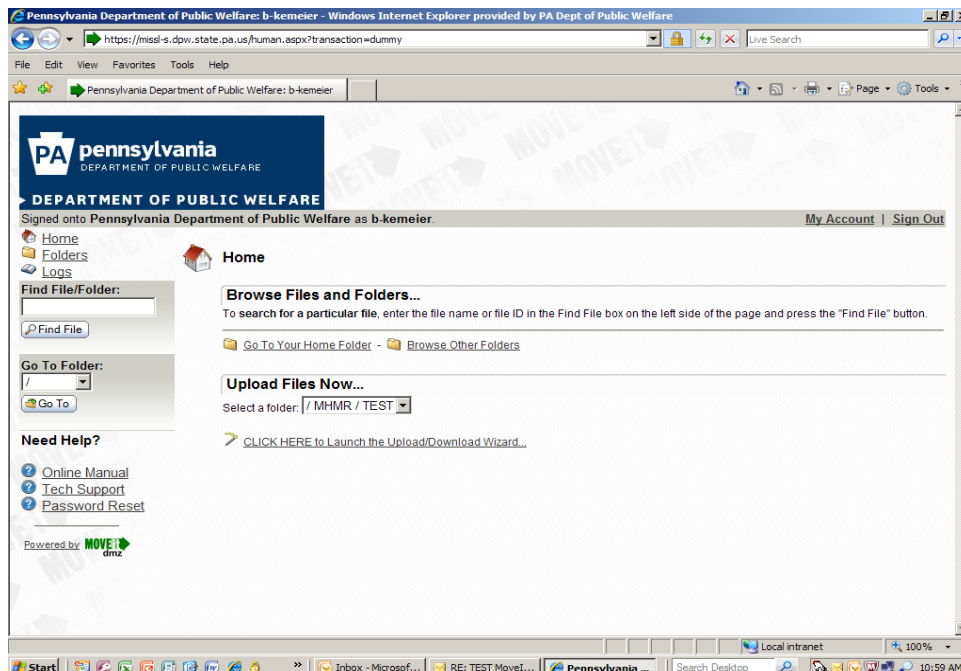
Installation of ActiveX

Home Page - Wizard Install

The first time a user signs on to MOVEit DMZ, MOVEit DMZ will notice that the Upload/Download Wizard is not installed, and will send the user to a page from which they can install the Wizard, or choose to disable it.

Internet Explorer (XP and Windows 7)

Internet Explorer users will be sent to the ActiveX Wizard Installation page, which gives options to install the ActiveX Wizard, disable it, or disable it and install the Java Wizard. **NOTE:** User must have "Administrator" rights to perform this task; If unable to install Active X – contact local IT support and request Administrator to install.

If you choose Try to install, you will be sent to a page which will attempt to download the ActiveX control. This may take several seconds. You may need to alter your browser's security settings to permit signed ActiveX controls to be installed in order to successfully complete the process.

If you choose Disable, you will not be prompted to install the ActiveX Wizard again unless you explicitly request it via the Account Options page. If you choose Disable (this session only), during the next browser session, you will be shown a link to install the Wizard.

If you have trouble installing ActiveX, you can go to the "Tools" menu on the Internet Explorer tool bar (at the top of the screen), and then click Internet Options, Security, and then "Sites". A list of existing trusted sites will appear and your MOVEit DMZ site should be listed in the "Add this website to the zone" text box. Click the "Add" button to finish trusting your MOVEit DMZ site, and use the "Close" and "OK" buttons to leave the window behind.

When complete, you should see a "Trusted sites" label (with a green checkmark) in place of the "Internet" label (with the globe) at the bottom of your IE browser window.
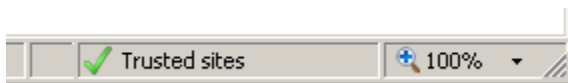
Internet Explorer 7.0 (on Windows Vista)

If you are running Internet Explorer 7.0 on Windows Vista, you may have to perform an extra step before you can use all the features of the Wizard, such as the ability to download multiple files at once. This extra step is to add any MOVEit DMZ site you communicate with into your Internet Explorer list of "Trusted Sites".

To change your security settings in this way, double-click on the "Internet" label (with the globe) at the bottom of your IE browser window.

An "Internet Security Properties" dialog window will be displayed. Click the "Trusted Sites" icon (the green checkmark) and then click the "Sites" button. A list of existing trusted sites will appear and your MOVEit DMZ site should be listed in the "Add this website to the zone" text box. Click the "Add" button to finish trusting your MOVEit DMZ site, and use the "Close" and "OK" buttons to leave the window behind.
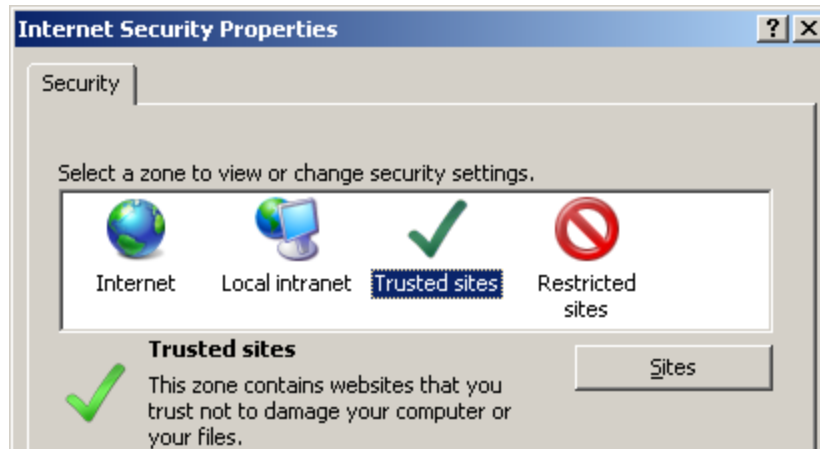
When complete, you should see a "Trusted sites" label (with a green checkmark) in place of the "Internet" label (with the globe) at the bottom of your IE browser window.
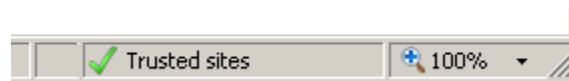
Other Browsers

The first time a user signs on to MOVEit DMZ with a browser other than Internet Explorer (e.g. Firefox), MOVEit DMZ will display a slightly different page with a link to install the Java Upload/Download Wizard. The Java Upload/Download Wizard is a component very similar to the ActiveX Wizard, designed for environments that can't run ActiveX controls.
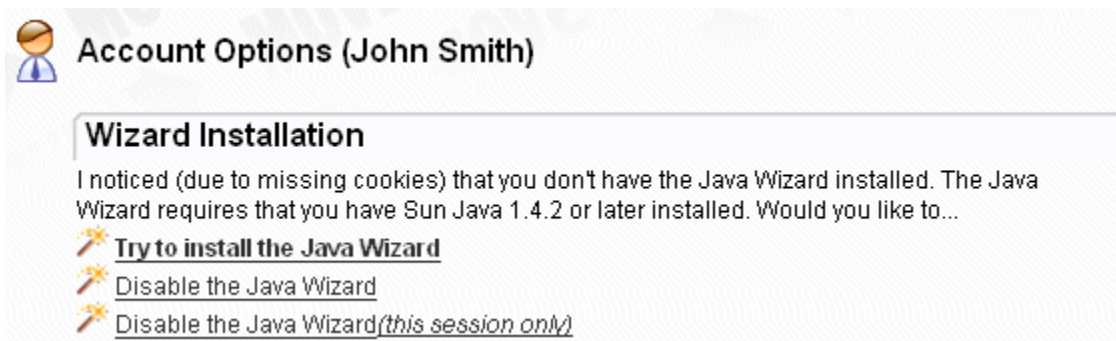
The choices are similar to those for the ActiveX Wizard. If Java is not installed, the user can simply choose Disable to avoid being prompted to install the Java Wizard in subsequent sessions.

Java can be downloaded from Sun's Java website. Select Java version 1.4.2 or higher for your PC.

Download New Files

After signing onto the SeGov website, user will see an SeGov "**Home**" page.
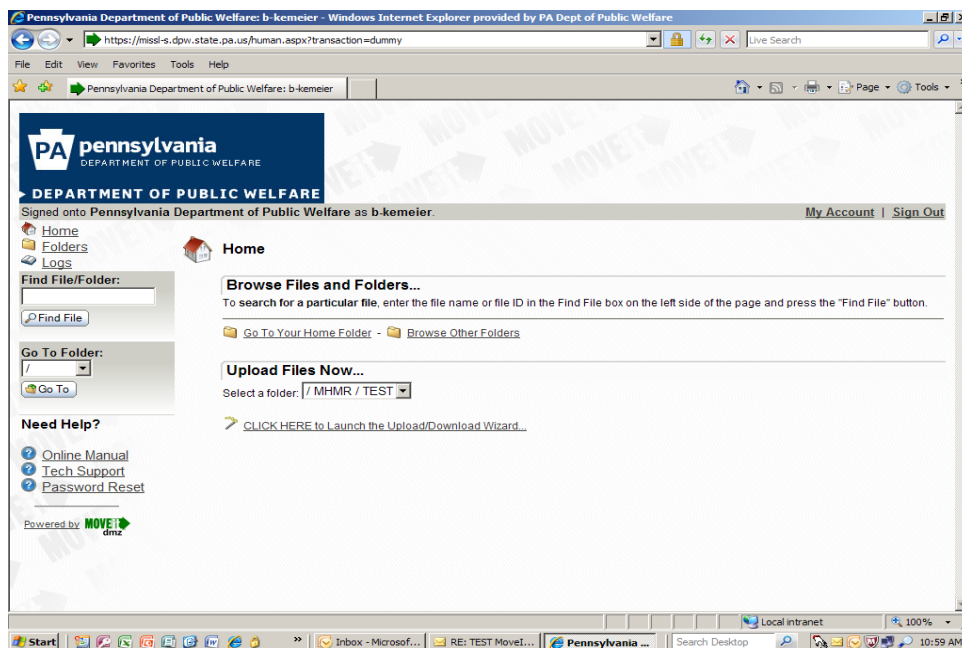
Under **Browse Files and Folders**, click "**Go to Your Home Folder**". User will be sent to their SeGov "**Home**" folder, which is also called their SeGov "**Parent**" folder (as seen in the screen below).
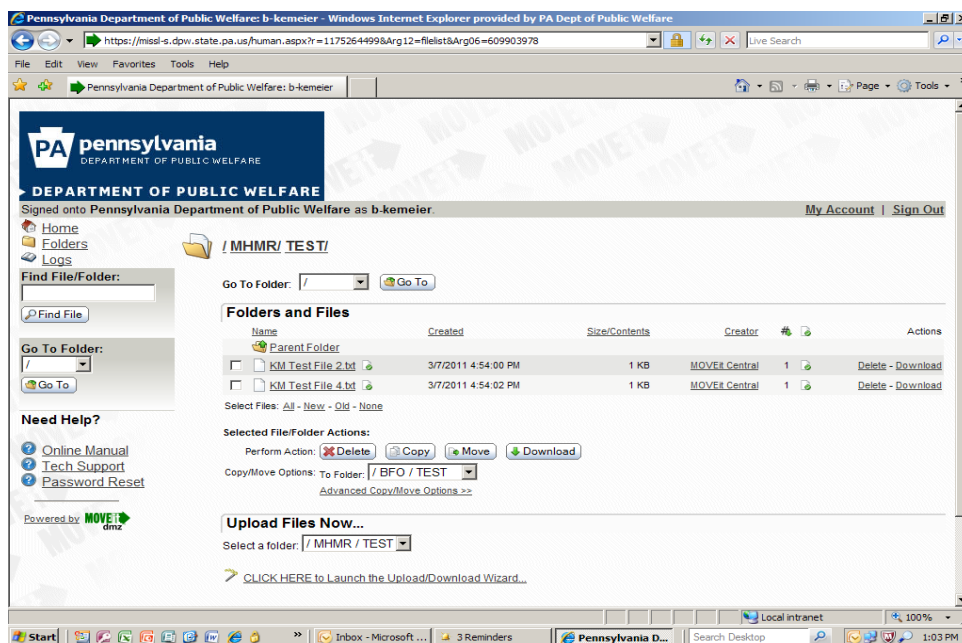
In the screen above, files available for download will be displayed in a Business Entity folder, which is one-level below your "**parent**" folder (or if you have multiple applications, there will be Business Entity

folders under each "**parent**" folder that you have access to). In the screen above, the "**parent**" folder is called "**MHMR**". Under MHMR, there is a Business Entity folder called "**TEST**". The files available for download are in the Business Entity folder called "**TEST**". Note that the user may have multiple Parent folders, each with their own Business Entity folders.
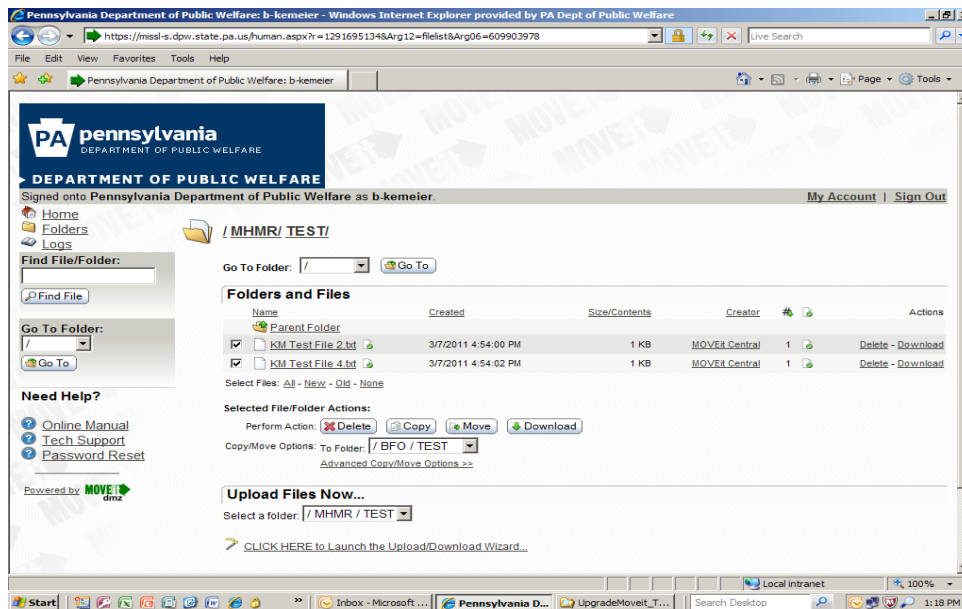
To download both of the files in the screen above, click the boxes to the left of each file name (in the screen above) and then click the "**Download**" button in the **Selected File/Folder Actions** section. This action will display the screen below.
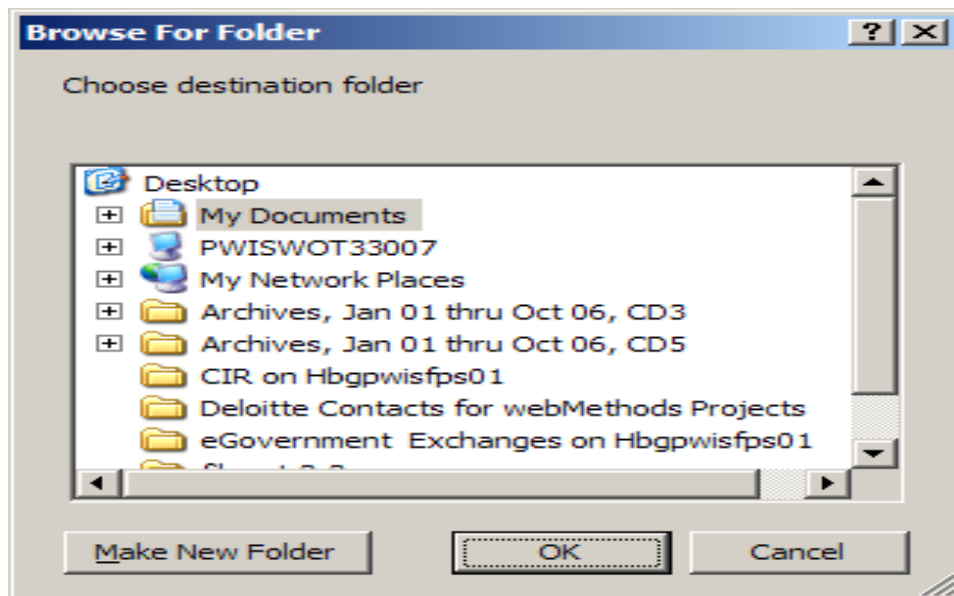
Navigate to the folder on your computer (or network) where files are to be placed. Then click **OK**.

The screen below indicates the file transfer was completed. Click **Open Folder** to see the files in your computer.
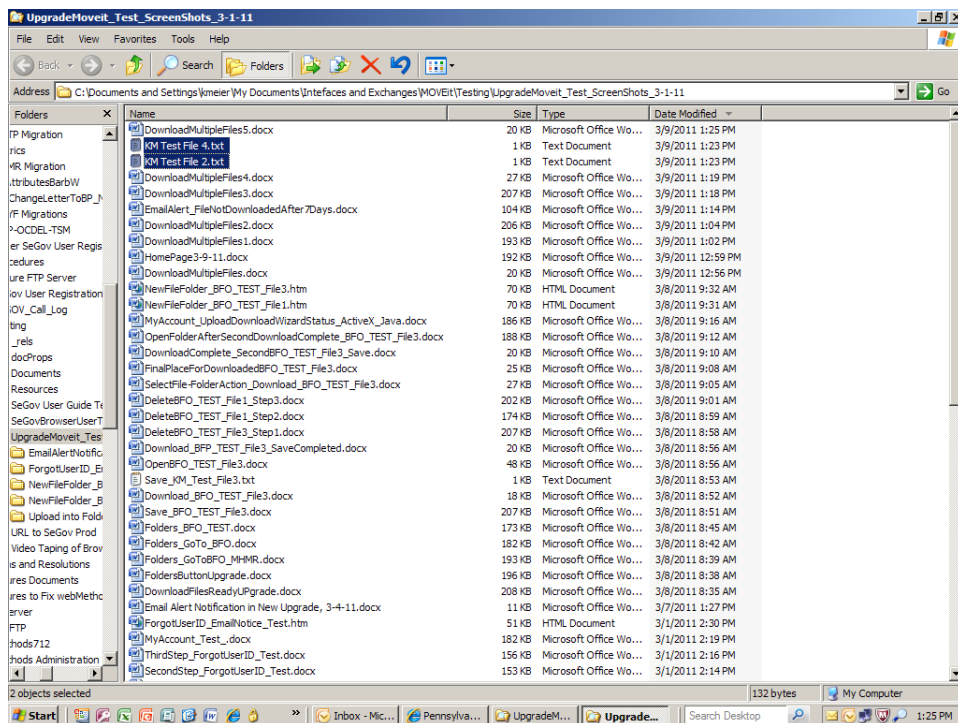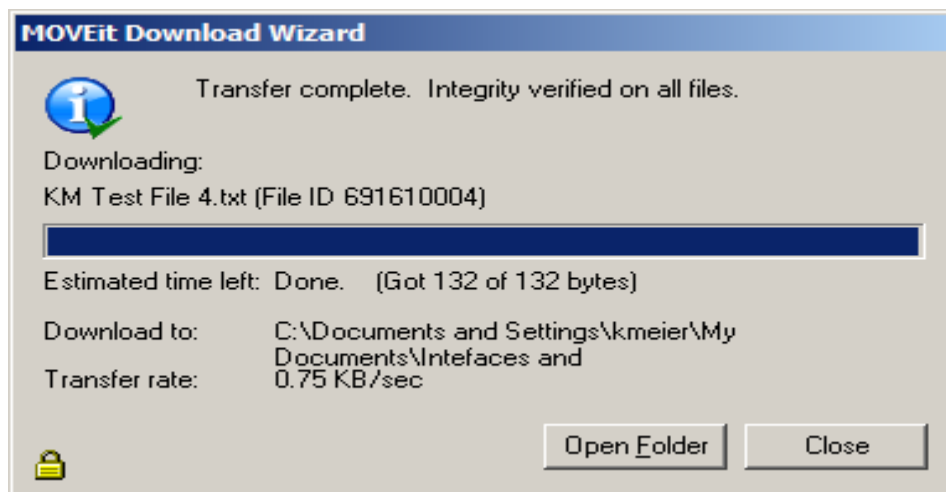
Notice the two files that were downloaded are highlighted on the screen above to show you that these are the files you downloaded above. Double click on each file to open up the files.

After the user has looked at the files, close the window and you will to return to the SeGOV screen below.
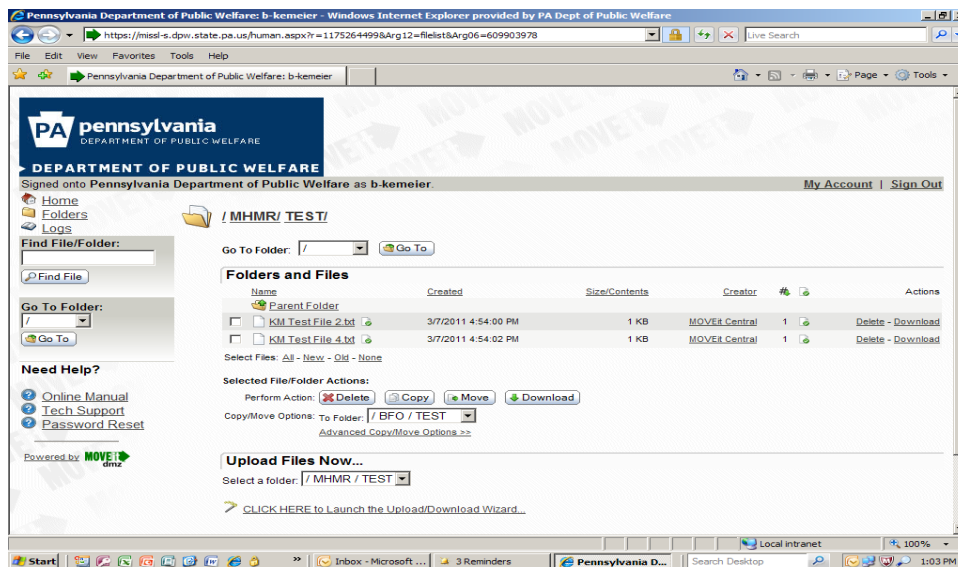
Delete Files that have been Downloaded

After downloading files, SeGov requires that Users maintain their site and delete files from the SeGov Site after download. New files with the same name *will not* be posted to the site until the existing file has been deleted.   SeGOV folders are **NOT** intended to be storage areas for Business Partner Files.

The User will be notified by email that file has not been downloaded within 7 days.

Files will be removed from the SeGOV after 30 days. All requests for files to be resent MUST be directed to DPW Program Office coordinator.

To maintain their SeGov Home page and **DELETE** files that have been downloaded, click the boxes to the left of each file name (in the previous screen above) and then click the "**Delete**" button in the **Selected File/Folder Actions** section. Now you will see the screen below:
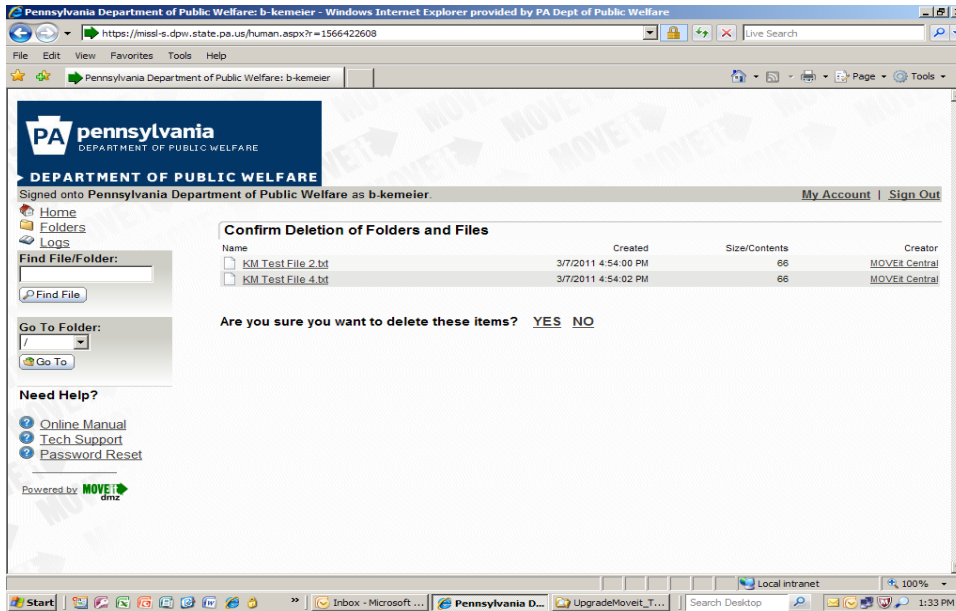
A file mask will be displayed in the screen above. The question, "**Are you sure you want to delete these files**" will be asked. Now do either of the following actions:

Click "**Yes**" and your file will be deleted.

Click "**No**" and your file will NOT be deleted.

The screen below confirms that you have deleted the two files.
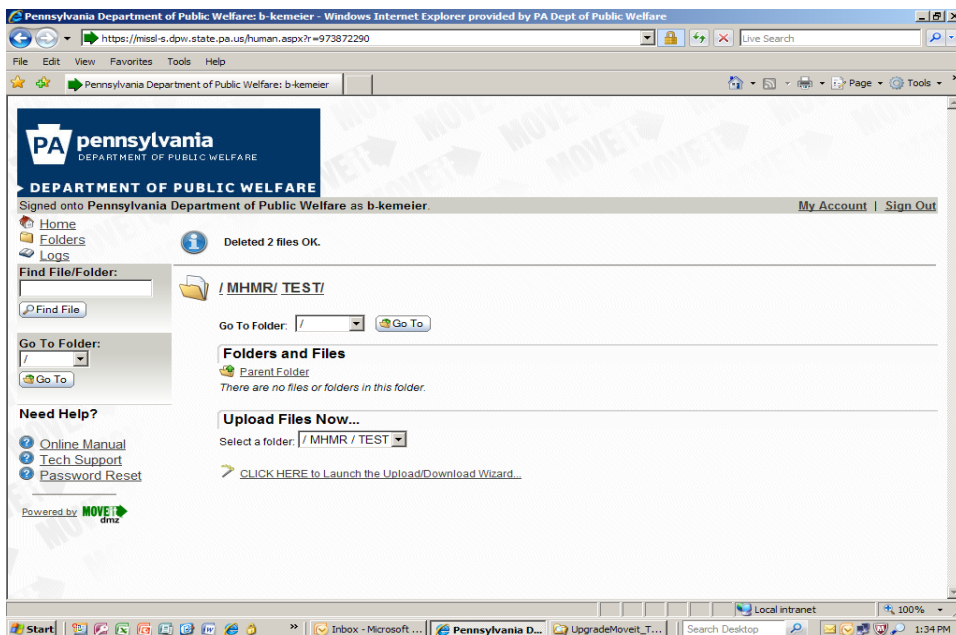
My Account

The user can click "**My Account**" on their SeGov **Home** page.

User can **NOT** change their email address here. Submit email address changes to the DPW Program Office Coordinator.
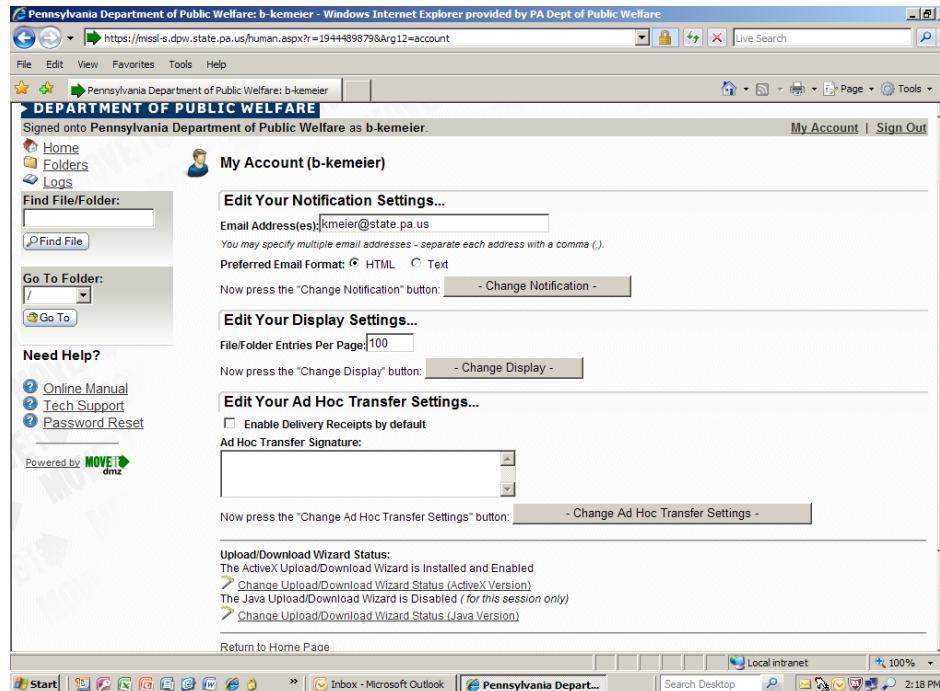
Access to Multiple Folders

One user may have access to multiple folders.

It is VERY important that files be uploaded to the proper folder with the proper file name. SeGOV team *will not* move files that have been uploaded incorrectly.

SeGOV allows one user to access multiple folders. This can be accomplished in several ways:

- From list of options at the left side of the Home page, click "**Folders**".
- From Home page, navigate to "**Browse Files and Folders**" section and then click on "**Browse other Folders**".
- From "**Find File/Folder**" link at the left side of the Home page: In the field, enter the name of the file, followed by a forward slash (/), and then enter the name of the folder. Then click "**Find File**".

Upload Files

If user is required to send files to DPW, start with the "**Upload Files Now**" section of their SeGov **Home** page.

It is **VERY** important that files be uploaded to the proper folder with the proper file name. SeGOV team *will not* move files that have been uploaded incorrectly. In the **Upload Files Now** section, click the drop-down arrow to select the folder that you want the file to be uploaded to. In the screen below, the folder was selected as MATP/TEST.
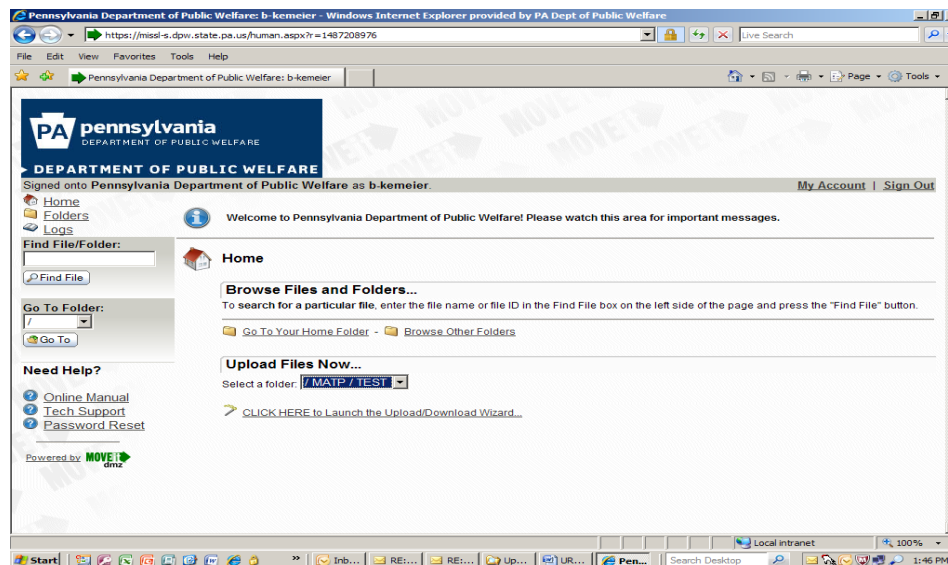
Then click "**Click Here to Launch Upload Wizard**" on the same screen. Upload wizard screen will be displayed. Select **Add File** in the screen below (DO **NOT** select Add **Folder** – SeGOV may experience difficulties accessing user defined folders).
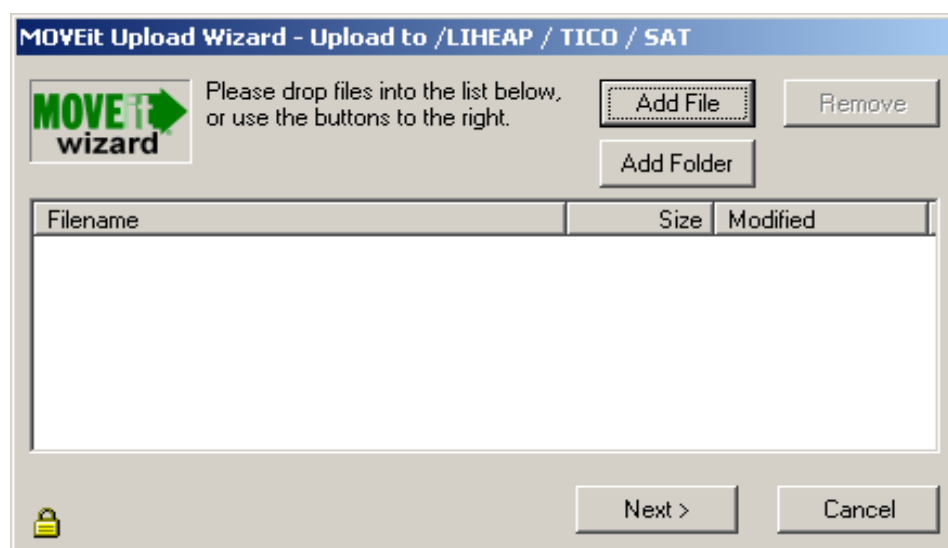
Select a file to be uploaded from user computer or network by finding it in your computer or network (similar to the screen below) and then double click on the file name.
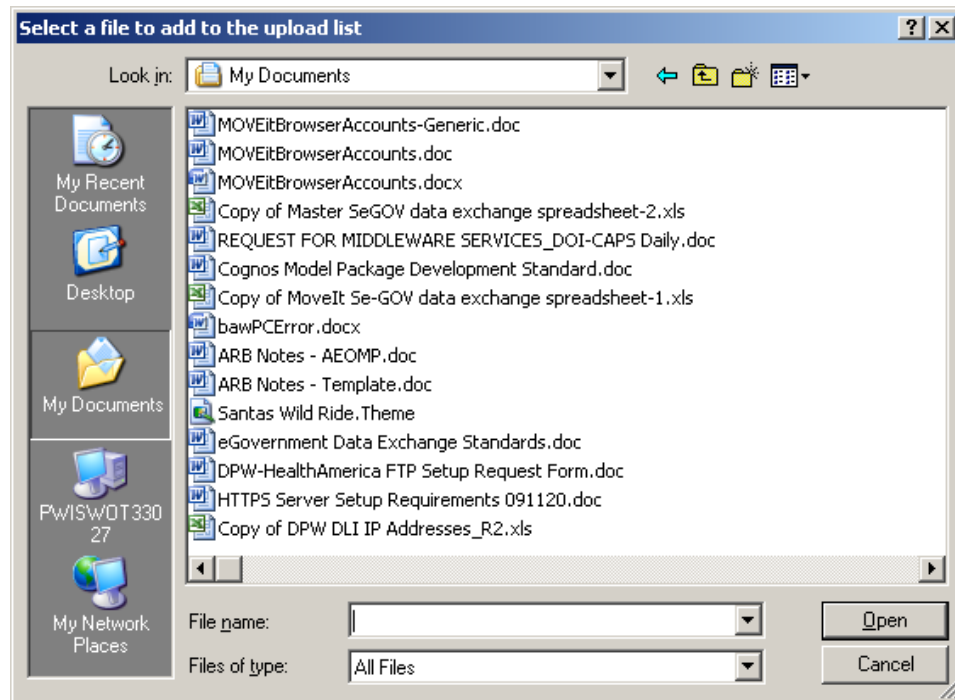
The location of the file on your computer or network, and the file name, will both appear as one "address" in the field called, "**Filename**", in the screen at the bottom of page 31. Click **Next** to continue.
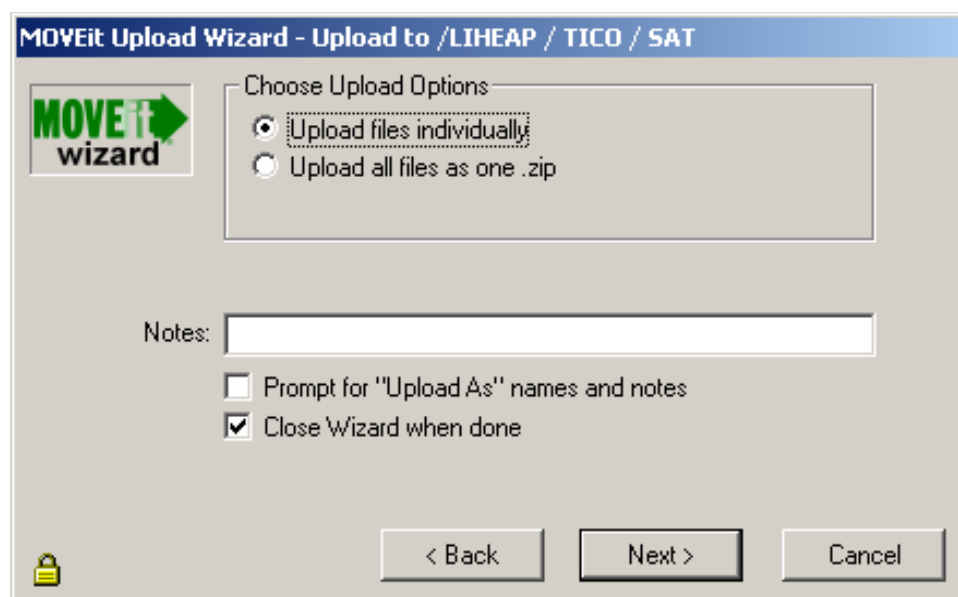
Click **Next** (all defaults are used)
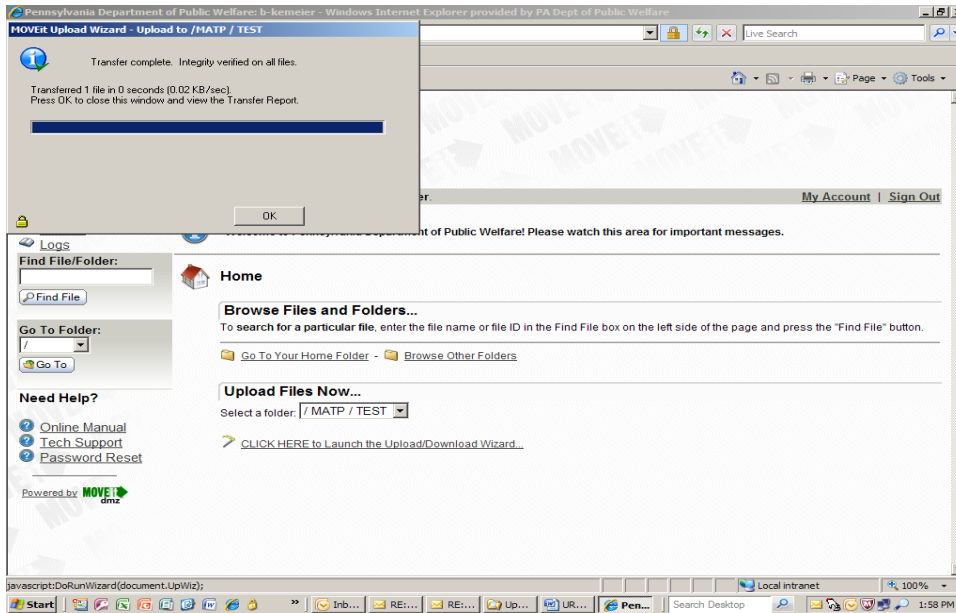
File Upload is verified in the small dialog box at the upper-left part of the screen above.

Click OK to complete the file transfer and you will return to your SeGov **Home** page.

Review the **Upload Wizard Transfer Report** on the screen below (at the bottom of the **Home** page).
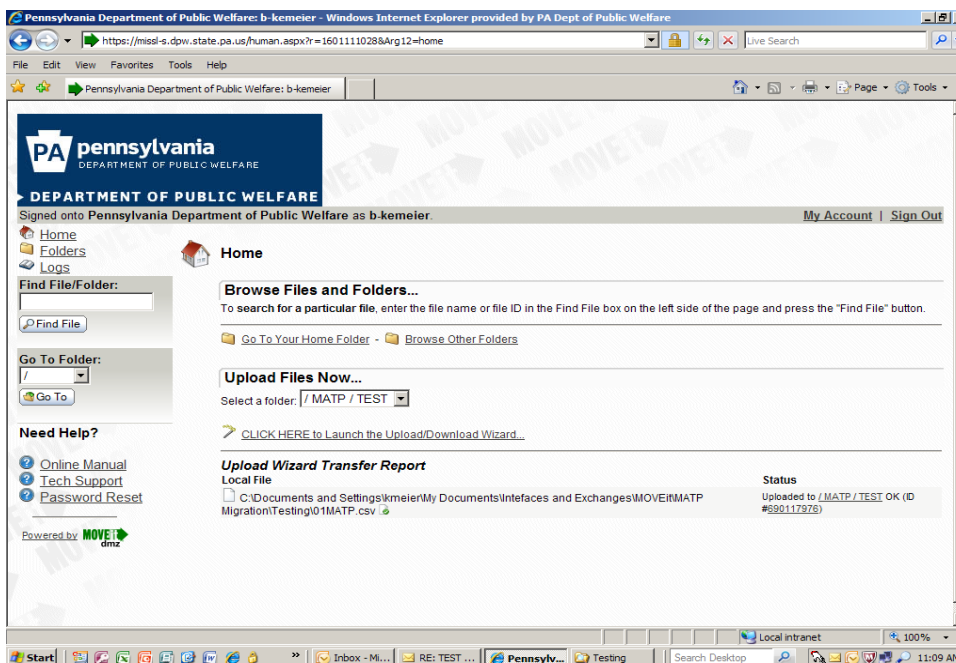
Note: Files are transferred based on standard file naming patterns. If the file remains in this directory 24 hours later, there is a problem. Review the defined file naming pattern, or contact your Program Office coordinator.

The user will receive an Email Alert Notification (like the one below) that your file has been uploaded to SeGov.
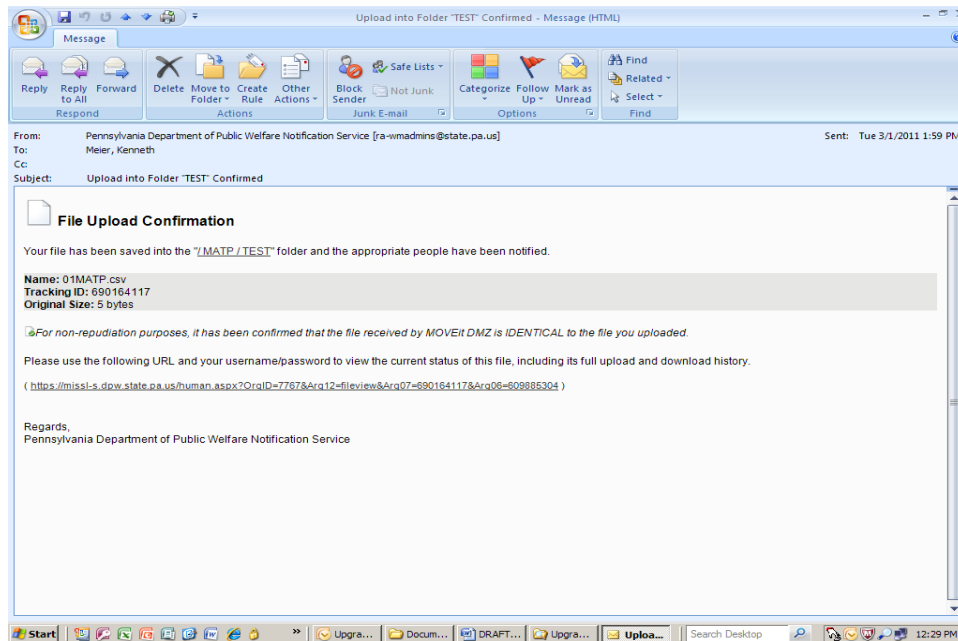
End Session

Per Commonwealth policy, Secure eGovernment browser sessions will time-out from non-use. When your session is complete, remember to "**Sign Out**" of the SeGov server (by clicking the "**Sign Out**" button in the upper right-hand part of any SeGov screen).

MANAGEMENT DIRECTIVE

COMMONWEALTH OF PENNSYLVANIA

GOVERNOR'S OFFICE

Subject: Commonwealth of Pennsylvania Information Technology Acceptable Use Policy
By Direction Of: Joseph S. Martz, Secretary of Administration, Bureau of Enterprise Architecture, OA, (717) 772-8062

1. PURPOSE. This policy is established to provide Authorized Users with guidelines for, restrictions upon and standards for acceptable use of Commonwealth IT resources. All Authorized Users must be familiar with this policy and adhere to it.

2. BACKGROUND. The Commonwealth of Pennsylvania has established a complex enterprise network of IT resources that connects agency networks with the Internet and other business partner networks for the purpose of sharing and accessing information in accordance with the mission of the Commonwealth. Commonwealth workforce members, including employees, contractors, consultants, volunteers and other Authorized Users, are expected to use this network and its connected IT resources in accordance with authorized job functions and in accordance with the acceptable use guidelines documented in this directive.

It is the policy of the Commonwealth to ensure that all Authorized Users that have access to Commonwealth IT resources are made aware of and comply with the standards set forth in this directive and in Enclosures 1 and 2. These standards encourage effective use of IT resources and provide a framework to prevent misuse or illegal use of these resources. This directive does not prohibit employees from performing authorized job duties.

3. SCOPE. This directive applies to all Authorized Users in all agencies under the Governor's jurisdiction who have access to Commonwealth IT resources.

4. POLICY.
a. These standards are designed to prevent use that may be illegal, abusive, or which may have an adverse impact on the Commonwealth or its IT resources and to identify permissible and effective uses. Authorized Users are encouraged to assist in the enforcement of these standards by promptly reporting any observed violations to their supervisor, the human resources office, agency contact or contracting officer.

205.34 Amended

This directive establishes policy for the acceptable use of Commonwealth information technology (IT) resources, including of the Internet and electronic mail (E-mail) by Commonwealth workforce members, including employees, contractors,consultants, volunteers and other authorized users (hereinafter referred to as Authorized Users). Marginal dots have been excluded due to major changes. March 28, 2007

b. The improper use of Commonwealth IT resources by employees or volunteers may result in disciplinary action, up to and including termination, depending on the circumstances of the incident. The improper use of Commonwealth IT resources by contractors or consultants may result in disciplinary action that may include formal action under the terms of the applicable contract or debarment under the

Contractor Responsibility program. When warranted, the Commonwealth or its agencies may pursue or refer matters to other authorities for criminal prosecution against persons who violate local, state, or federal laws through the use of Commonwealth IT resources.

c. Authorized Users of Commonwealth IT resources should be aware that all records of computer use, Internet use and/or E-mail communication (sent, received, or stored) conducted on Commonwealth IT resources are the property of the Commonwealth. Individual Authorized Users do not control access to such records. At its discretion, executive level or Human Resources staff or their authorized designees may access and review any computer files or data, Internet records or E-mail communications for compliance with the provisions of this directive. Agency heads may determine who may access these records, including, but not limited to, executive level staff, legal staff, human resource management staff, network system administrators, individuals in the Authorized User's chain of command or others, including law enforcement. Files and records of IT resource use may be reviewed at any time and are routinely backed up and stored without the user's knowledge. All physical equipment, intellectual property, information, software, data, files or programs that are provided, stored or otherwise utilized by or on any Commonwealth-provided IT resource is the property of the Commonwealth.

d. All Authorized Users should understand that all electronic communication and access may be traced and/or monitored. Agencies and their designees may use tracking, blocking, and monitoring software to restrict certain access and/or alert information technology staff to certain inappropriate uses. Authorized Users must use passwords and/or encryption in a manner that is consistent with Commonwealth and agency policy. Utilization of special passwords or encryption does not necessarily guarantee the confidentiality of any electronic communication. Authorized Users must keep passwords secure and must not share them with others.

e. The Internet and E-mail are information tools that the Commonwealth has made available on Commonwealth computer resources for Commonwealth business purposes. Where personal use of these resources does not interfere with the efficiency of operations and is not otherwise in conflict with the interests of the Commonwealth, reasonable use of the Internet and/or E-mail for personal purposes will be permitted in accordance with standards established for business use. Such personal use shall be limited, occasional, and incidental. Any personal use which is inconsistent with Commonwealth policy regarding availability or capability of computer equipment, or inappropriate content of communications as defined by this policy, is prohibited.

f. All existing employees must be provided a copy of this policy. All new employees must review this policy during new employee orientation. All non-employee Authorized Users must review this policy prior to their use of Commonwealth IT resources.

g. As acknowledgement of receipt and understanding of this policy, agencies must obtain a signed user agreement in the form of Enclosure 2 from each Authorized User who has been granted access to Commonwealth IT resources. Agencies must obtain a signed user agreement from each new employee prior to granting such employee access to Commonwealth IT resources. Agencies may continue to use existing user agreements for ninety (90) days after the issue date of this Directive, but thereafter agencies may only grant access to Commonwealth IT Resources to Authorized Users who had signed a user agreement in the form of Enclosure 2, unless a waiver of this requirement has been granted by the Office of Administration.

h. Each agency must maintain copies of the agreement signed by each user authorized by the agency. Completed user agreements shall be maintained as part of the employee's Official Personnel Folder. Alternately, users may sign and agencies may store these agreements in an electronic format consistent with *Management Directive 210.12, Electronic Commerce Initiatives and Security, and ITB—SEC006, Commonwealth of Pennsylvania Electronic Signature Policy*. Signed agreements must be accessible to individuals who are authorized to view or use the documents.

Appendix 1, Page 3 of 3

i. Technical standards for use of the Commonwealth IT resources will be published in Office of Administration/Office for Information Technology (OA/OIT) "IT Bulletins" that will be available on the OA/OIT Internet site at <http://www.oit.state.pa.us>.

j. Requests for records pertaining to Commonwealth IT resources must be addressed consistent with all laws, directives or policies that would apply to the same information if maintained in a non-electronic format. These requests should be referred to agency legal counsel.

k. This policy supplements and where conflicting, supersedes *Management Directive 205.29, Commonwealth Internet Access.*

l. This policy supersedes any existing IT, Internet and/or E-mail use policy issued by agencies under the Governor's jurisdiction that is inconsistent with this directive, unless specific exemptions are granted by the Secretary of Administration or designee. Approved labor agreements or "side letters" should be read in a manner to effectuate both this policy and any such agreement or letter. In cases where a provision of an approved labor agreement or "side letter" cannot be reconciled with this policy, the labor agreement or side letter will control. Agencies may develop supplemental IT, Internet and/or E-mail policies only with the approval of the Secretary of Administration or designee. Agencies must ensure that Authorized Users with access to Commonwealth IT resources have access to this directive and Enclosures 1 and either Enclosure 2 or Enclosure 3, as appropriate, either electronically or in hard copy. All use of Commonwealth IT resources must conform with Executive Order 1980-18, Code of Conduct, Management Directive 505.7, Personnel Rules, and Commonwealth policies on nondiscrimination and sexual harassment.

Appendix 1 ENCLOSURES:
1 – Commonwealth Acceptable Use Standards for Information Technology (IT) Resources

2 – Commonwealth Acceptable Use Policy Agreement Commonwealth Employee or Volunteer Form
3 – Commonwealth Acceptable Use Policy Agreement Commonwealth Contractor or Consultant Form
This directive supersedes *Management Directive 205.34*, dated September 12, 2000.

Appendix 1, Enclosure 1 to Management Directive 205.34 Amended, Page 1 of 6:

COMMONWEALTH ACCEPTABLE USE STANDARDS FOR INFORMATION TECHNOLOGY (IT) RESOURCES

Each Authorized User must comply with these standards when using the Internet or Commonwealth IT resources.

AUDITING AND REPORTING
The Commonwealth reserves the right to monitor and/or log, with or without notice, all Internet activity, all Internet web site access, all E-Mail and any other communications or data accessed, stored or otherwise used by or on Commonwealth IT resources. Therefore, Authorized Users should have no expectation of privacy in the use of the Commonwealth's IT resources. Authorized Users are encouraged to assist in the enforcement of these standards by promptly reporting any observed violations to their supervisor, the human resources office, agency contact or contracting officer. All physical equipment, intellectual property, information, software, data, files or programs that are provided, stored or otherwise utilized by or on any Commonwealth IT resource is the property of the Commonwealth.

DISCIPLINE
Misuse of Commonwealth IT resources by employees or volunteers may result in disciplinary action, up to and including termination, depending on the circumstances of the incident. The improper use of Commonwealth IT resources by contractors or consultants may result in disciplinary action that may include formal action under the terms of the applicable contract or debarment under the Contractor Responsibility program. When warranted, the Commonwealth or its agencies may pursue or refer matters to other authorities for criminal prosecution against persons who violate local, state, or federal laws through the use of Commonwealth IT resources.

GENERAL IT RESOURCE USE
a. As part of the privilege of being an Authorized User, Authorized Users may not attempt to access any data or programs contained on Commonwealth systems for which they do not have authorization or explicit consent.

b. Authorized Users may not share their Commonwealth or agency account(s), passwords, Personal Identification Numbers (PIN), Security Tokens (i.e. Smartcard), or similar information or devices used for identification and authorization purposes with any other person or Authorized User. Authorized Users are strictly responsible for maintaining the confidentiality of their Commonwealth or agency account(s), passwords, PIN, Security Tokens or similar information or device.

c. Authorized Users may not make unauthorized copies of copyrighted software.

d. Authorized Users may not use non-standard shareware or freeware software without agency IT management approval unless it is on the agency's standard software list.

e. Authorized Users may not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of IT Resources; deprive an Authorized User of access to an IT resource; obtain extra IT Resources beyond those allocated; or circumvent computer security measures.

Appendix 1, Enclosure 1 to Management Directive 205.34 Amended, Page 2 of 6:

f. Authorized Users may not use Commonwealth IT resources for personal gain.

g. Authorized Users may not engage in illegal activity in connection with their use of Commonwealth IT Resources, including, but not limited to downloading, installing or running security programs or utilities that reveal or exploit weaknesses in the security of a system. For example, Authorized Users may not run password cracking programs, packet sniffers, port scanners or any other non-approved programs on Commonwealth IT resources unless they are specifically authorized to do so.

h. Authorized Users may not intentionally access, create, store or transmit material that is generally considered to be inappropriate or personally offensive, including sexually suggestive, pornographic or obscene material.

i. Authorized Users may not utilize unauthorized proprietary and/or commercial Instant Messaging (IM) products on Commonwealth computer resources. Refer to *Management Directive 210.15 – Instant Messaging.*

j. Authorized Users are personally responsible for the security of authorized portable Commonwealth IT resources such as issued laptops, Blackberries and cell phones. Care must be exercised to ensure these devices are not lost, stolen or otherwise accessed in an unauthorized manner.

k. Authorized Users may not store non-public information on IT resources, if those IT resources will be removed from Commonwealth facilities without prior approval from the agency Secretary or designee.

l. Authorized Users may only use encryption methods approved by the Commonwealth to encrypt information.

m. Authorized Users may not use non-Commonwealth or non-approved storage devices or storage facilities without the approval of the agency Secretary or designee.

INTERNET USE
All security policies of the Commonwealth and its agencies, as well as policies of Internet sites being accessed, must be strictly adhered to by Authorized Users.

Software
In connection with Authorized Users' use of and access to Commonwealth IT Resourses:

a. All software used to access the Internet must be part of the agency's standard software suite or approved by the agency IT department. This software must incorporate all vendor provided security patches.

b. All files downloaded from the Internet must be scanned for viruses using the approved Commonwealth distributed software suite and current virus detection software.

c. All software used to access the Internet shall be configured to use an instance of the Commonwealth's standard Internet Access Control & Content Filtering solution.

Expectation of Privacy
a. Authorized Users may not rely on any communications via the Internet using Commonwealth IT Resources being secure, private, or inaccessible, except where appropriate security applications are used, e.g. data encryption.

b. All activity on Commonwealth IT resources is subject to logging and review.
Enclosure 1 to Management Directive 205.34 Amended Page 3 of 6

Access Control and Authorization

Agencies should authorize access to the Internet using Commonwealth computer resources through the utilization of a user ID/password system. Security violations can occur through unauthorized access and all possible precautions should be taken to protect passwords. Authorized Users are responsible for activity and communications transmitted under their account.

Incidental Use

a. Use of Commonwealth IT resources is only authorized for personal use on a limited, occasional, and incidental basis and in a manner consistent with this policy.

b. Incidental personal use of Internet access is restricted to Authorized Users; it does not extend to family members or other acquaintances.

c. Access to the Internet from an agency owned, home based computer must adhere to all the same policies that apply to use from within agency facilities. Employees may not allow family members or other non-employees to access agency computer systems.

d. Incidental use must not result in direct costs to the Commonwealth.

e. Incidental use must not interfere with the normal performance of an Authorized User's work duties.

f. No user may send or solicit files, documents or data that may risk legal liability for, or embarrassment to, the Commonwealth.

g. All files and documents located on Commonwealth IT resources, including personal files and documents, are owned by the Commonwealth and may be accessed in accordance with this policy. In addition, it should be understood that such documents may be subject to the Right to Know Law 65 P.S. § 66.1, *et seq.* and other laws that may require the Commonwealth to disclose the content of its IT resources.

Acceptable Use of the Internet

Accepted and encouraged use of the Internet for Authorized Users on Commonwealth IT Resources includes, but is not limited to, the following:
1. Access, research, exchange, or posting of information that relates to the assigned job duties of an Authorized User for carrying out Commonwealth business.

2. Promotion of public awareness in regard to Commonwealth law, agency services, and public policies.

3. Posting of agency information that has been authorized by appropriate management.

E-MAIL USE
Expectation of Privacy

a. When sensitive material is sent electronically via E-mail, it is important to verify that all recipients are authorized to receive such information and to understand that E-mail is not fully secure and/or private, except where appropriate security applications are used, e.g. data encryption.

b. Users should understand that messages can be quickly and easily copied and may be forwarded inappropriately.

c. Where it is necessary to transmit Commonwealth proprietary or restricted information beyond the Commonwealth Connect E-mail network, the messages should be protected by encryption. Authorized Users should contact their agency network coordinator or Information Technology Coordinator for assistance if encryption is needed.

Appendix 1, Enclosure 1 to Management Directive 205.34 Amended, Page 4 of 6:

d. E-mail messages to be transmitted outside of the United States should comply with local laws governing international transmission of data as well as United States export control regulations. For assistance, Authorized Users should contact their network coordinator or Information Technology Coordinator, who may receive technical assistance from the Office of Administration, Office for Information Technology.

e. The agency head or designee should determine specific agency policy regarding business information which is determined to be too confidential or sensitive to be transmitted via E-mail.

f. All user activity on Commonwealth IT resources is subject to logging and review.

Access Control and Authorization
a. Only Authorized Users may use Commonwealth IT resources to send or view E-mail or access the Commonwealth's E-mail systems.

b. Unauthorized persons may not use the network or Commonwealth equipment to originate E-mail messages or read E-mail messages directed to others.

c. Access Commonwealth E-mail will only be granted to Commonwealth workforce members, including employees, contractors, consultants, volunteers and other authorized users if they agree to abide by all applicable rules of the system, including this policy and its related standards.

d. Unauthorized access of an Authorized User's E-mail files is a breach of security and ethics and is prohibited. An Authorized User may not access the E-mail or account of another Authorized User unless granted permission to do so by the Authorized User. This restriction does not apply to system administrators and management staff in the Authorized User's chain of command who are authorized to access E-mail for legitimate business purposes.

e. In accordance with agency policy, Authorized Users should use password protection to limit access to E-mail files. Authorized Users must safeguard their passwords so that unauthorized users do not have access to their E-mail. Authorized Users are responsible for messages transmitted under their account.

Message Retention
E-mail messages may be subject to Commonwealth and/or agency document retention standards. See *Management Directive 210.5 Records Management* for additional guidelines.

E-mail Security Issues – Worms & Viruses
E-mail and attachments to E-mail increasingly are reported to be sources of computer viruses. All Authorized Users should act in accordance with the latest Information Technology Bulletins regarding containment methods for computer viruses.

Maintaining Professionalism.
Every Authorized User who uses Commonwealth computer resources is responsible for ensuring posted messages are professional and businesslike. As a way to impose personal restraint and professionalism, all employees should assume that whatever they write may at some time be made public. Authorized Users should follow the following guidelines:
1. Be courteous and remember that you are representing the Commonwealth with each E-mail message sent.

2. Review each E-mail message before it is sent and make certain that addresses are correct and appropriate.

Appendix 1, Enclosure 1 to Management Directive 205.34 Amended, Page 5 of 6:

3. Consider that each E-mail message sent, received, deleted, or stored has the potential to be retrieved, seen, and reviewed by audiences, including the general public, who were not the intended recipient of the message.

4. Ensure that content is appropriate and consistent with business communication; avoid sarcasm, exaggeration, and speculation which could be misconstrued.

5. Be as clear and concise as possible; be sure to clearly fill in the subject field so that recipients of Email can easily identify different E-mail messages. Avoid subject fields that are vague and general, e.g. "question," "comment," etc.

Electronic Message Distribution, Size and Technical Standards
a. Authorized Users should receive authorization from their chain supervisor before wide scale "broadcasting" an E-mail bulletin to groups of employees.

b. The use of "reply to all" should be avoided unless it is appropriate to respond to all addressees.

c. Authorized Users wishing to send E-mail bulletins to all Commonwealth or agency employees must first obtain authorization from agency management.

d. E-mail messages should be brief, and attachments to E-mail messages should not be overly large. Agency IT staff will inform Authorized Users of limitations on the size of E-mail messages and attachments. The Office for Information Technology periodically will provide technical standards and guidance to agencies through IT Bulletins on the technical capacities of the Commonwealth Connect system and limitations on Email message size. Technical standards will be provided in areas such as file size and backup procedures, and will be available on the OA/OIT Internet site at **<http://www.oit.state.pa.us>.**

UNACCEPTABLE USES OF IT RESOURCES
The following are examples of impermissible uses of Commonwealth IT resources. This list is by way of example and is not intended to be exhaustive or exclusive. Authorized Users are prohibited from:
1. Viewing, accessing, posting or transmitting any material that is generally considered to be personally offensive or inappropriate, including sexually suggestive, pornographic, or obscene materials.

2. Viewing, accessing, posting or transmitting material that expresses or promotes discriminatory attitudes toward race, gender, age, nationality, religion, or other groups including, but not limited to, protected groups identified in *Executive Order 1996-9, Equal Employment Opportunity.*

3. Conducting personal, for-profit transactions or business or conducting any fundraising activity not specifically sponsored, endorsed, or approved by the Commonwealth.

4. Participating in Internet activities that inhibit an employee's job performance or present a negative image to the public, such as auctions, games, accessing pornographic or offensive material, or any other activity that is prohibited by directive, policy or law.

5. Attempting to test or bypass the security ("hacking" or "cracking") of computing resources or to alter internal or external computer security systems.

6. Participating in or promoting computer sabotage through the intentional introduction of computer viruses, worms or other forms of malware, i.e. malicious software.

7. Promoting, soliciting or participating in any activities that are prohibited by local, state, or federal law or the Commonwealth rules of conduct.

Appendix 1, Enclosure 1 to Management Directive 205.34 Amended, Page 6 of 6:

8. Violating or infringing the rights of any other person.

9. Using any other Authorized User's password and/or equipment to conduct unacceptable activities on Commonwealth IT Resources.

10. Harassing or threatening activities including, but not limited to, the distribution or solicitation of defamatory, fraudulent, intimidating, abusive, or offensive material.

11. Transmitting or soliciting any proprietary material, such as copyrighted software, publications, audio or video files, as well as trademarks or service marks without the owner's permission.

12. Promoting or participating in any unethical behavior or activities that would bring discredit on the Commonwealth or its agencies.

13. Downloading and/or installing any unapproved software.

14. Transmitting or posting any messages that intentionally misrepresent the identity of the sender, hide the identity of the sender, or alter a sender's message.

15. Sending or forwarding confidential or sensitive Commonwealth information through non-Commonwealth email accounts. Examples of non-Commonwealth email accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers.

16. Sending, forwarding or storing confidential or sensitive Commonwealth information utilizing non-Commonwealth accredited mobile devices. Examples of mobile devices include, but are not limited to, Personal Data Assistants, two-way pagers and cellular telephones.

17. Participating in any other Internet or E-mail use that is deemed inappropriate by the Commonwealth and/or its agencies and is communicated as such to Authorized Users.

COMMONWEALTH IT RESOURCE ACCEPTABLE USE POLICY USER AGREEMENT – COMMONWEALTH EMPLOYEE OR VOLUNTEER

This user agreement does not prohibit employees from performing authorized job duties.
I have read the attached Management Directive _____, "*Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*" and in consideration of the Commonwealth of Pennsylvania making its IT Resources available to me, I agree to abide by the requirements set forth therein. I understand that disciplinary action, up to and including termination, may be taken if I fail to abide by any of the requirements of this agreement. I further understand that my Commonwealth IT resource usage may be monitored at any time and by signing this Agreement, I specifically acknowledge such monitoring. I further understand that if I have any questions regarding this Directive, I am required to ask for clarification from my supervisor or my agency Human Resource representative.

Printed Name: _____

Employee Number: _____

Signature: _____

Date: _____

Agency: _____

Bureau/Facility: _____

Division/Section: _____

Mailing/E-mail Address: _____

Work Phone: _____

Optional Agency Approval: _____

Date: _____

COMMONWEALTH IT RESOURCE ACCEPTABLE USE POLICY USER AGREEMENT – COMMONWEALTH CONTRACTOR OR CONSULTANT
This user agreement does not prohibit contractors or consultants from performing services required by their contract with the Commonwealth.

I have read the attached Management Directive _____, "*Commonwealth of Pennsylvania Information Technology Acceptable Use Policy*" and in consideration of the Commonwealth of Pennsylvania making its IT Resources available to me, I agree to abide by the requirements set forth therein. I understand that the Commonwealth may take appropriate action, including any action specified in my contract with the Commonwealth, as well as under the Commonwealth's Contractor Responsibility Program, if I fail to abide by any of the requirements of this agreement. I further understand that my Commonwealth IT resource usage may be monitored at any time and by signing this Agreement, I specifically acknowledge such monitoring.

Printed Name: _____

Contractor: _____

Signature: _____

Date: _____

Contracting Agency: _____

Bureau/Facility: _____

Division/Section: _____

Mailing/E-mail Address: _____

Work Phone: _____

Optional Agency Approval: _____

Date: _____

Federal ID #: _____

Mailing Address: _____

E-mail address: _____

Work Phone: _____

Signature: _____