Office of Administrative Hearings (OAH) **Procedures Transmittal**			**Transmittal Number:** 10-01
Distribution:			**Date:** June 2, 2010 **Page:** 1 of 2 plus 5-Page Attachment
ALB OAH Staff ☒	**UPS ALJs** ☒	**Upstate LDSS** ☐	**Subject:**
	SUP ALJs ☒		**OAH Email Encryption Procedures**
NYC OAH Staff ☒	**NYC ALJs** ☒	**NYC Agencies** ☐	
	SUP ALJs ☒		

The Office of Administrative Hearings (OAH) has conducted a review of our policies concerning email that contains confidential information. Based on this review, we are implementing new procedures, on a pilot basis, that will make such emails secure by encrypting them during their transmission. The need to encrypt email that is sent from OAH is primarily the responsibility of staff in the Communications Intake Unit who respond to emails, faxes, correspondence and telephone inquiries from appellants and representatives, as well as staff handling litigation matters. However, these procedures must be followed by all OAH staff when sending an email containing confidential information to any individual[s] outside the NYSEmail Global directory.

Effective immediately, OAH will use Microsoft Exchange Hosted Encryption (EHE) for all emails that contain confidential information and that are being sent to non-NYSEmail Global directory addressees. This service encrypts OAH's outgoing emails and attachments and stores them on a secure server. By entering a password, the addressee can then retrieve the message from that server and, when necessary, send an encrypted response.

If the intended recipient of an email containing confidential information is not included in the NYSEmail global directory, OAH staff must encrypt that email. This is accomplished by including the word ENCRYPT followed by a colon (":") anywhere in the Subject line of the email message, as follows: "Encrypt:"--include the colon but not the quotes.

When the OAH staff member sends the encrypted email, the recipient will receive an email indicating that the sender has sent an encrypted email. To view the email, the recipient must click on the attachment to this message, which is named "message_zdm.html." After the recipient enters his/her password (see below), the encrypted email will be displayed and any attachments to the email will be available.

The recipient may respond to this email when it is displayed by clicking the "Reply," "Reply All," or "Forward" button, and that response or forwarded email will also be encrypted.

NOTE: Messages will only remain open for 15 minutes before timing out. After that, the recipient must log back into the server and reopen the message to redisplay it.

In order to retrieve an encrypted email from the secure server, a user who is not on the NYSEmail system must first establish a password. The user will be prompted to create a password the first time a message is retrieved. This password should be retained by the user as it can then be used to retrieve any other encrypted mail from OAH. A "Forgot Password" prompt is available.

Please note, if the email is sent to an address listed in the NYSEmail global directory, the email will not be encrypted, even if the subject line has the word "ENCRYPT:" in it.

Appendix I contains detailed instructions about establishing a password and about sending and receiving encrypted emails using EHE.

Appendix II contains OTDA's definitions of confidential and non-confidential information.

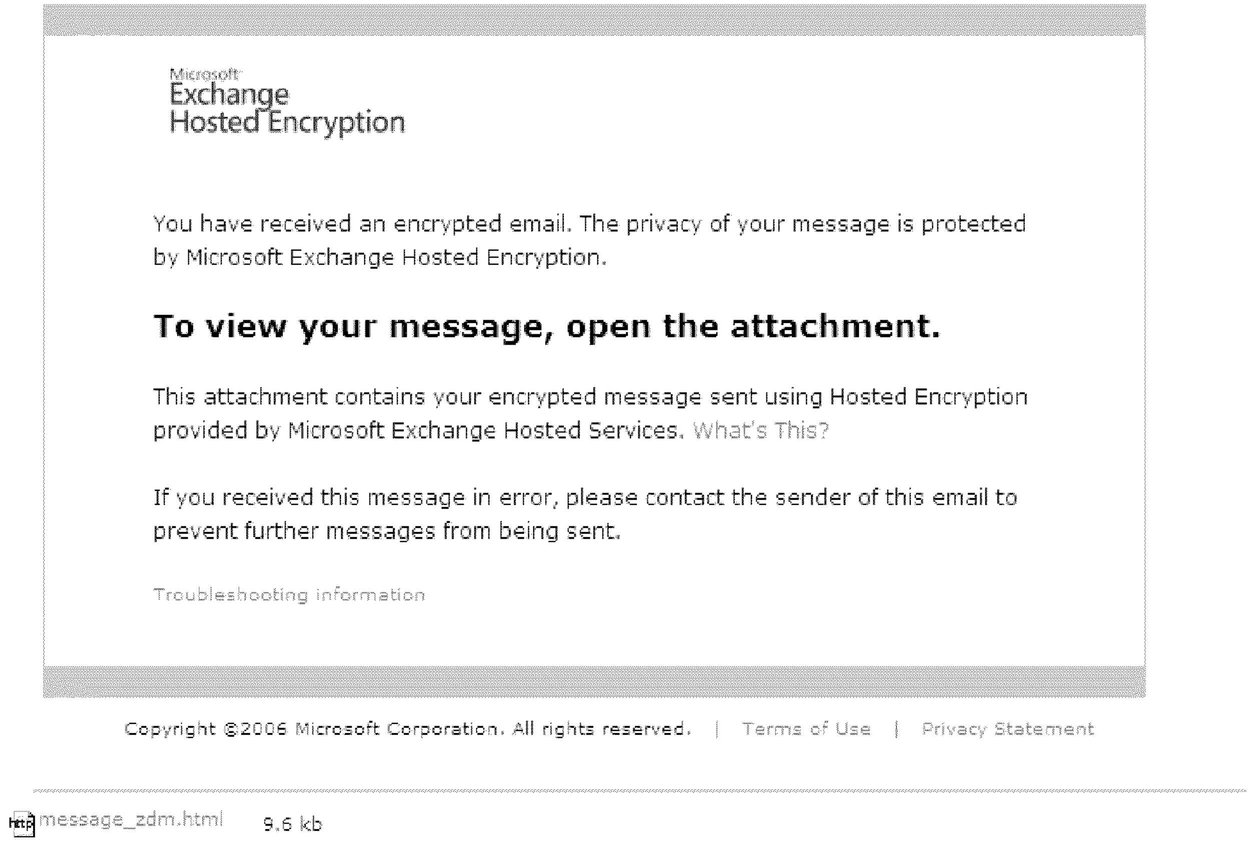
If you have any questions regarding this transmittal, you may contact your supervisor or The System Help Desk at 1-866-396-6551 or via e-mail at helpme@otda.state.ny.us .

Susan Fiehl

Susan Fiehl, Assistant Director of Administration
Office of Administrative Hearings

APPENDIX I: DETAILED INSTRUCTIONS TO RETRIEVE AN ENCRYPTED EMAIL

1. If you are not in the NYSEmail global directory and you open an encrypted email, you will see the following message. Click on the link for the attachment. It is entitled "message_zdm.html."



Microsoft
Exchange
Hosted Encryption

You have received an encrypted email. The privacy of your message is protected by Microsoft Exchange Hosted Encryption.

To view your message, open the attachment.

This attachment contains your encrypted message sent using Hosted Encryption provided by Microsoft Exchange Hosted Services. What's This?

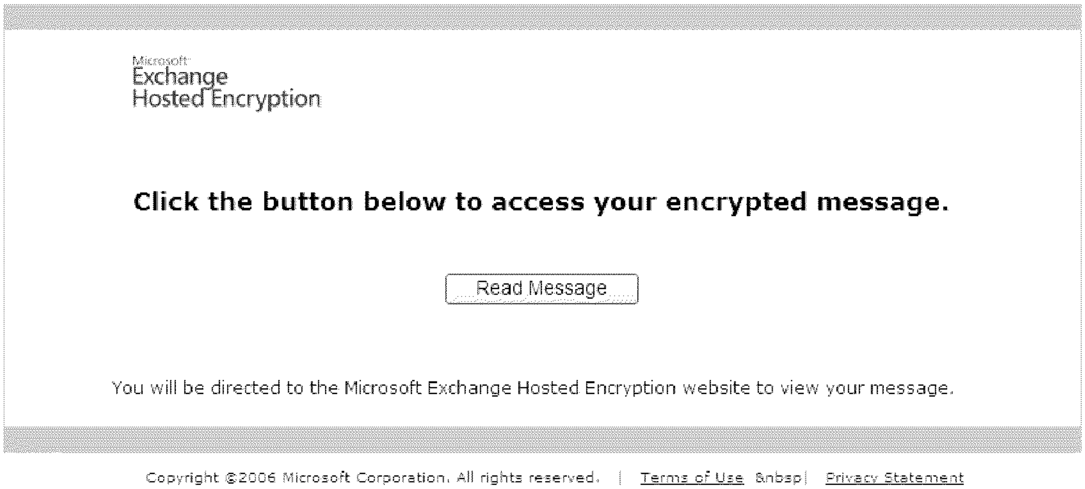
If you received this message in error, please contact the sender of this email to prevent further messages from being sent.

Troubleshooting information

Copyright ©2006 Microsoft Corporation. All rights reserved. | Terms of Use | Privacy Statement

message_zdm.html 9.6 kb

2. The following screen will appear. Click on the “Read Message” button.

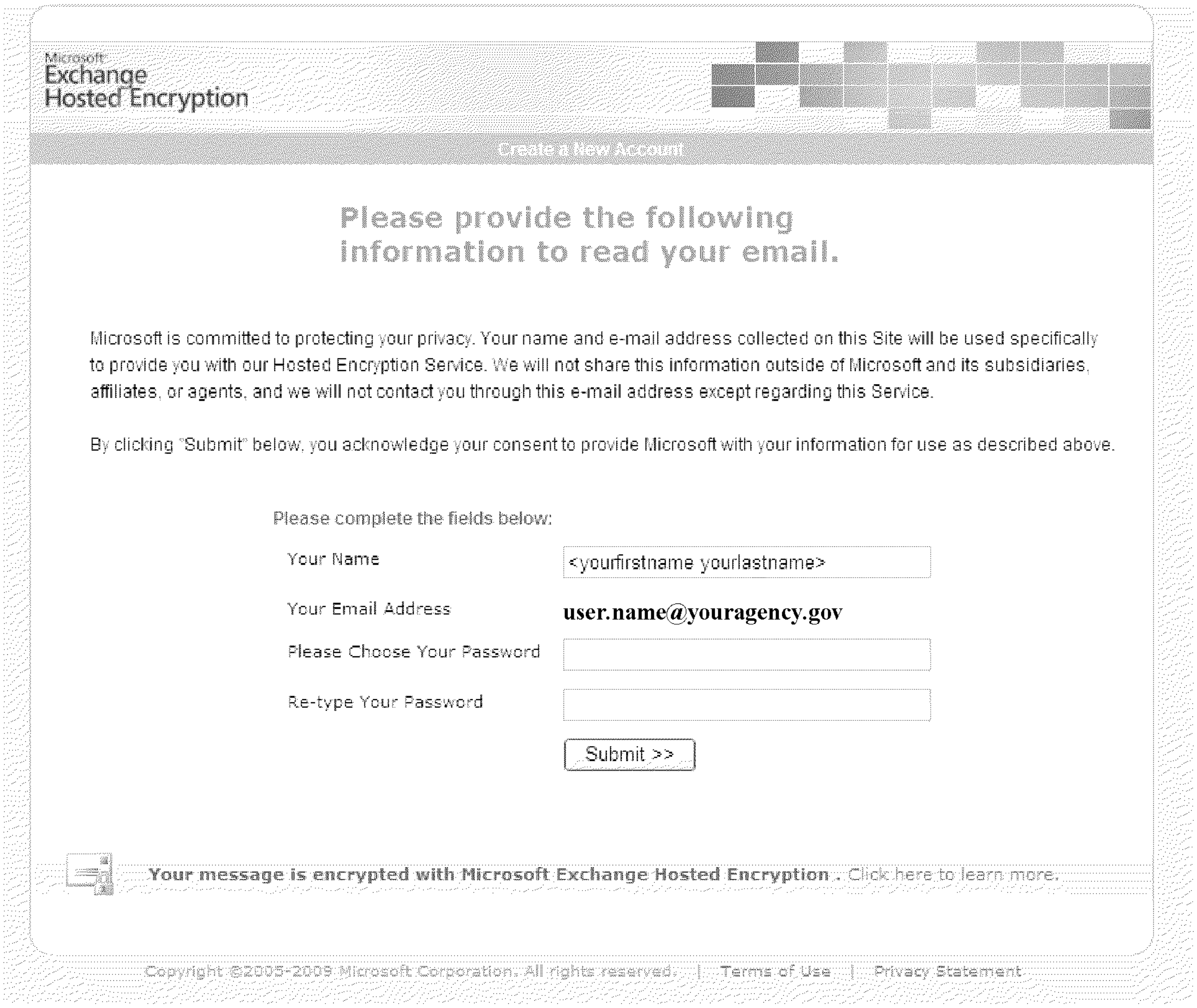


Click the button below to access your encrypted message.

You will be directed to the Microsoft Exchange Hosted Encryption website to view your message.

Copyright ©2006 Microsoft Corporation. All rights reserved. | Terms of Use | Privacy Statement

3. If you have never retrieved encrypted email from Microsoft Exchange Hosted Encryption Services before, you will be prompted to create a password on the following screen:



Please provide the following information to read your email.

Microsoft is committed to protecting your privacy. Your name and e-mail address collected on this Site will be used specifically to provide you with our Hosted Encryption Service. We will not share this information outside of Microsoft and its subsidiaries, affiliates, or agents, and we will not contact you through this e-mail address except regarding this Service.

By clicking "Submit" below, you acknowledge your consent to provide Microsoft with your information for use as described above.

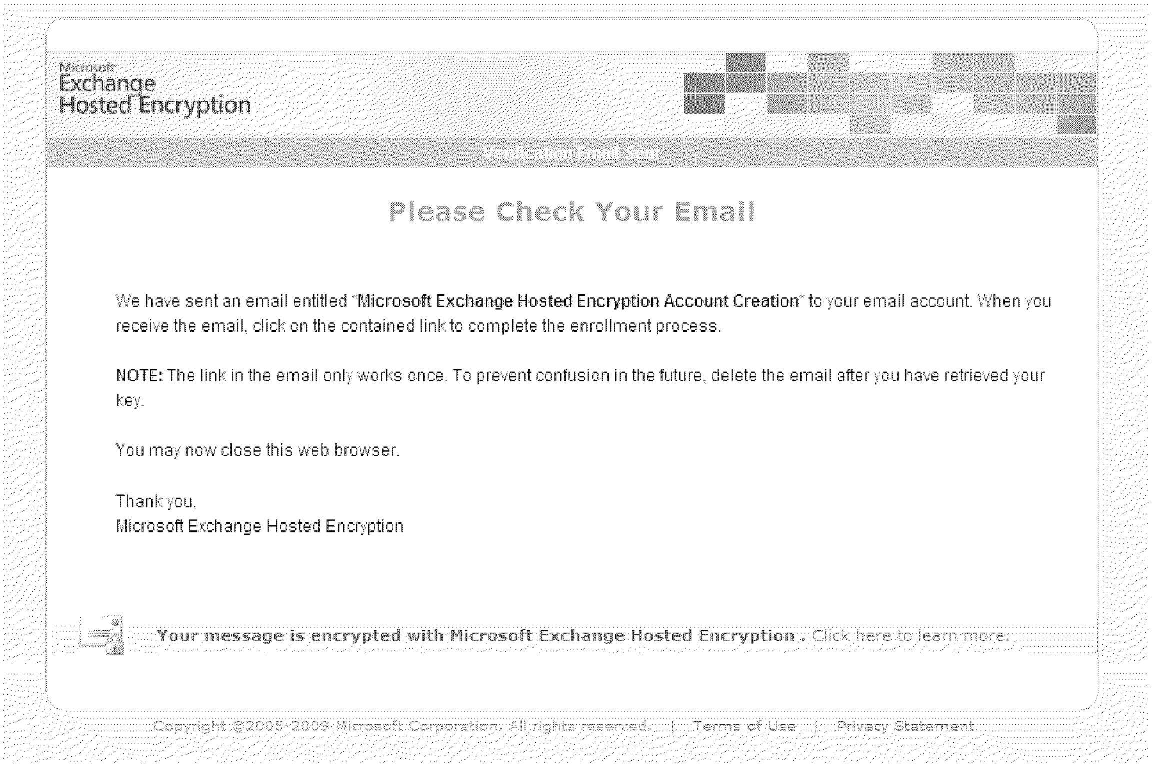
Please complete the fields below:

Your Name	<yourfirstname yourlastname>
Your Email Address	**user.name@youragency.gov**
Please Choose Your Password	
Re-type Your Password	

Your message is encrypted with Microsoft Exchange Hosted Encryption . Click here to learn more.

Copyright ©2005-2009 Microsoft Corporation. All rights reserved. | Terms of Use | Privacy Statement

4. After you create the password and click the Submit button, the following message, informing you to check your email, will appear:



Please Check Your Email

We have sent an email entitled "**Microsoft Exchange Hosted Encryption Account Creation**" to your email account. When you receive the email, click on the contained link to complete the enrollment process.

NOTE: The link in the email only works once. To prevent confusion in the future, delete the email after you have retrieved your key.

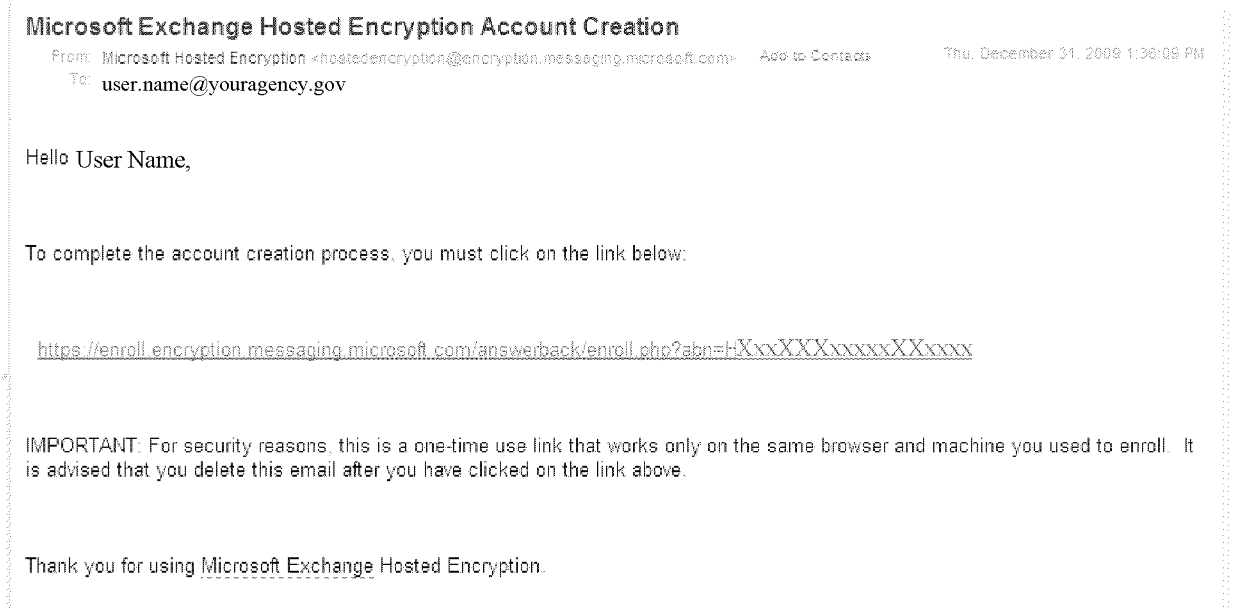
You may now close this web browser.

Thank you,
Microsoft Exchange Hosted Encryption

Your message is encrypted with Microsoft Exchange Hosted Encryption . Click here to learn more.

Copyright ©2005-2009 Microsoft Corporation. All rights reserved. | Terms of Use | Privacy Statement

5. In your email client (e.g., MS Outlook), open the email that you receive and click the link in the middle of the page to complete the account creation process. You will then be able to retrieve your email from the Microsoft Server.



Microsoft Exchange Hosted Encryption Account Creation

From: Microsoft Hosted Encryption <hostedencryption@encryption.messaging.microsoft.com> Thu, December 31, 2009 1:36:09 PM

To: user.name@youragency.gov

Hello User Name,

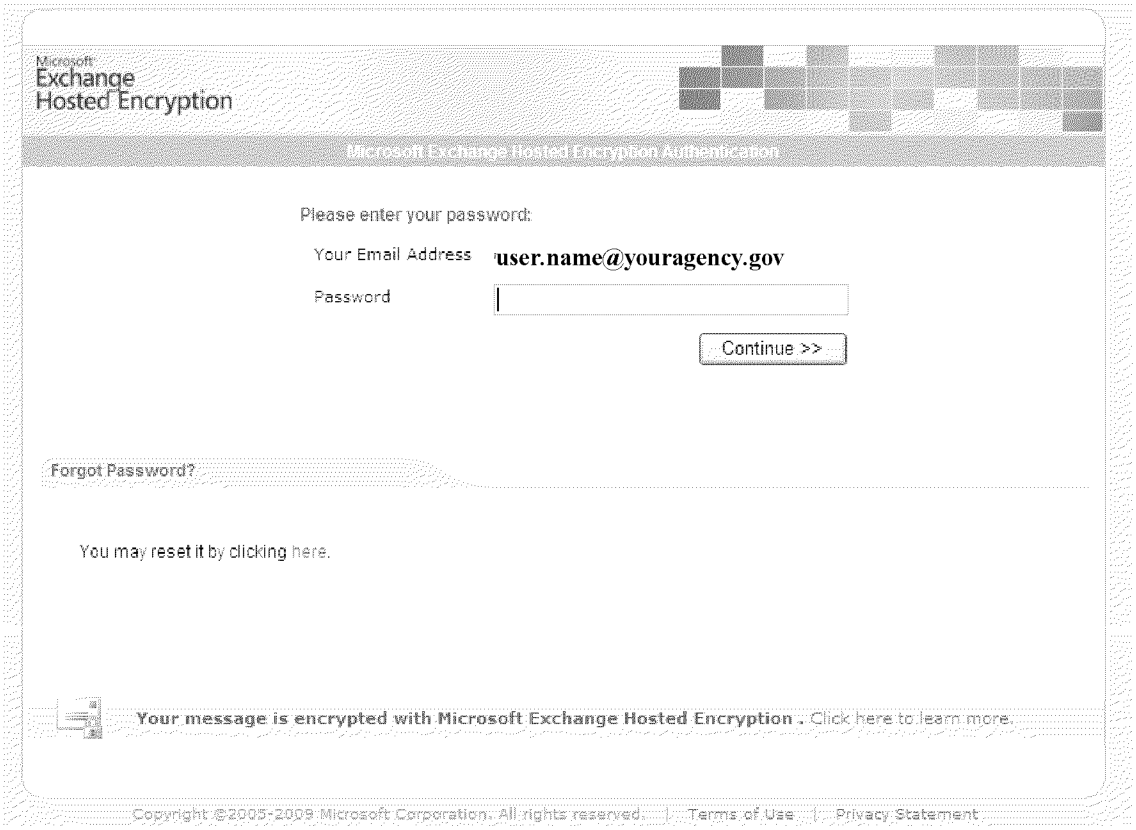
To complete the account creation process, you must click on the link below:

https://enroll.encryption.messaging.microsoft.com/answerback/enroll.php?abn=HXxxXXXxxxxxXXxxxx

IMPORTANT: For security reasons, this is a one-time use link that works only on the same browser and machine you used to enroll. It is advised that you delete this email after you have clicked on the link above.

Thank you for using Microsoft Exchange Hosted Encryption.

6. **Note that you only need to complete steps 3 through 5 ONCE**. After you have established your account, whenever you receive an encrypted email and click on the attachment ("message_zdm.html"), you will just need to enter the password you created. See the following screen:



Microsoft Exchange Hosted Encryption Authentication

Please enter your password:

Your Email Address user.name@youragency.gov

Password

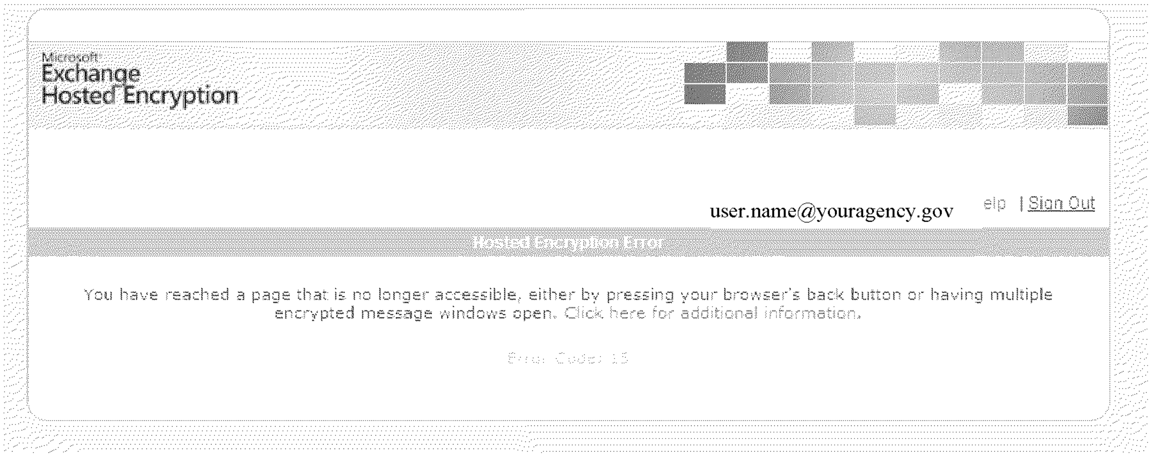
Forgot Password?

You may reset it by clicking here.

Your message is encrypted with Microsoft Exchange Hosted Encryption . Click here to learn more.

Copyright ©2005-2009 Microsoft Corporation. All rights reserved. | Terms of Use | Privacy Statement

Note: If your session lasts longer than 15 minutes, you will see the message below. You will need to access the original email and log in again.



user.name@youragency.gov

Hosted Encryption Error

You have reached a page that is no longer accessible, either by pressing your browser's back button or having multiple encrypted message windows open. Click here for additional information.

Error Code: 15

APPENDIX II: Definitions of Confidential and Non-Confidential Data

Chapter 4 of the New York State Office of Temporary and Disability Assistance Administrative Policies and Procedures Manual describes the general Office definitions of confidential and non-confidential data:

CONFIDENTIAL:

Client identifying/sensitive data--Client-identifying data whose use and dissemination are restricted by law to specific situations (e.g., Child Protective Services data).

Client identifying data--Any client-specific data which could identify individuals either currently or previously in receipt of or making application for assistance or services. Data regarding other individuals included in case records are confidential to the extent that they refer to individuals, e.g., persons paying child support. If normally non-confidential data, because of the size or characteristics of the population involved, could cause the identification of individuals then that data are also considered confidential. For example, the Office considers information about Fair Hearings decisions in Hamilton County to be confidential.

NYSOTDA personnel data--Data which identifies an individual and whose disclosure could result in an "unwarranted invasion of privacy" as defined under the Freedom of Information Act.

NYSOTDA policy/deliberative data--Information related to the official business of the Office whose disclosure could "impair a government process" as defined under the Freedom of Information Act.

NON-CONFIDENTIAL:

Non-identifying program or client data--Individual data which contains no specific identifying information.

Aggregate (statistical) data--Collective information developed from any source which could not identify, by inference, individuals.

"Administrative data"--Data created within NYSOTDA to support its responsibilities which, if available, must be released outside the Office under the Freedom of Information Act.

Provider data--Information identifying providers of services such as Shelter Services, vendors for contracted services, etc.