



Compliance Component

DEFINITION

<i>Name</i>	Web-based E-Mail Access
<i>Description</i>	Web-based E-mail Access is the ability to view, send and receive state e-mail from any location via the Internet using proper authentication. This compliance component defines the minimum guidelines when offering and securing access to state approved e-mail accounts via the world wide web through a web browser.
<i>Rationale</i>	Offers the ability to retrieve state e-mail remotely provided they have access to the Internet. Implemented improperly, access to state e-mail via the web, will compromise the integrity of state e-mail data and possibly the state's network and systems.
<i>Benefits</i>	<ul style="list-style-type: none"> • Ability to equip a remote work group with basic web access, reducing the cost for client machines and e-mail client licenses. • Reduced maintenance costs as there is no need to update e-mail client software. • No dedicated state client hardware required to provide access.

ASSOCIATED ARCHITECTURE LEVELS

<i>Specify the Domain Name</i>	Application
<i>Specify the Discipline Name</i>	Electronic Collaboration
<i>Specify the Technology Area Name</i>	E-mail Architecture
<i>Specify the Product Component Name</i>	

COMPLIANCE COMPONENT TYPE

<i>Document the Compliance Component Type</i>	Guideline
<i>Component Sub-type</i>	

COMPLIANCE DETAIL

<i>state the Guideline, Standard or Legislation</i>	Web-based E-Mail Access Criteria
	<ol style="list-style-type: none"> <u>Implementation Requirements</u> <ol style="list-style-type: none"> 1.1. Must be implemented on a hardened web server. The web server must have a secure connection to the E-mail Application Server. 1.2. The web server must be located in a DMZ and only appropriate ports permitted. 1.3. The mail server must not be located in the DMZ. <u>Security Requirements</u> <ol style="list-style-type: none"> 2.1. Must use minimum 128-bit encryption.

	<ul style="list-style-type: none"> 2.2. Must use HTTPS. 2.3. Must use state approved user authentication as defined in the MAEA Security Domain Architecture Blueprint. 2.4. Must provide a unique set of login credentials for web access to state e-mail accounts from outside the state network than those used to access state computing resources other than e-mail. 2.5. Must not use persistent cookies containing sensitive information. 2.6. Must maintain log of all web-based e-mail access. 2.7. Must have server-side anti-virus checking in place. 2.8. Should not be accessed by clients without appropriate and up-to-date anti-virus software. <p>3. <u>Browser Requirements</u></p> <ul style="list-style-type: none"> 3.1. Must support minimum 128-bit encryption. 3.2. Must support HTTPS. 3.3. Must use minimum level browser as required by the web e-mail application server. <p>4. <u>Usability Requirements</u></p> <ul style="list-style-type: none"> 4.1. Must be able to access and manage address books via web-based e-mail. 4.2. Must be able to manage messages (i.e., managing folders, views, forwarding, deleting, archival, etc.). 4.3. Must be able to send and retrieve e-mail attachments. 4.4. Should support spell checking of web-based e-mail. 4.5. Should be able to support proxy access. 4.6. Should be able to access public folders. 4.7. Should be able to save a copy of sent mail for retrieval at multiple locations. 4.8. Should offer access to calendaring and scheduling information.
<i>Document Source Reference #</i>	
Compliance Sources	
<i>Name</i>	
<i>Contact Information</i>	
<i>Name</i>	
<i>Contact Information</i>	
KEYWORDS	
<i>List Keywords</i>	HTTPS, SSL, Browser, web mail, web-mail, webaccess, web access, Internet mail, DMZ, iNotes, OWA
COMPONENT CLASSIFICATION	
<i>Provide the Classification</i>	<input type="checkbox"/> <i>Emerging</i> <input checked="" type="checkbox"/> <i>Current</i> <input type="checkbox"/> <i>Twilight</i> <input type="checkbox"/> <i>Sunset</i>
<i>Sunset Date</i>	

COMPONENT SUB-CLASSIFICATION

Sub-Classification	Date	Additional Sub-Classification Information
<input type="checkbox"/> <i>Technology Watch</i>		
<input type="checkbox"/> <i>Variance</i>		
<input type="checkbox"/> <i>Conditional Use</i>		

Rationale for Component Classification

Document the Rationale for Component Classification

Migration Strategy

Document the Migration Strategy

Impact Position statement

Document the Position statement on Impact

CURRENT STATUS

Provide the Current Status

In Development

Under Review

Approved

Rejected

AUDIT TRAIL

Creation Date

8/19/2003

Date Approved / Rejected

Reason for Rejection

Last Date Reviewed

Last Date Updated

Reason for Update