Introduction: Delegated User Access Authorization

• The three-step Request/Preauthorize/Approve Access process in MIDMS is replaced by a single Authorize Access action by the Identified Official with Authority (IOwA).

• The IOwA is appointed by the organization as responsible for assigning job duties. The IOwA role was rolled out to LEAs to authorize external access for all MIDMS-secured applications in Spring 2015. At LEAs, we recommend assigning the IOwA role to the superintendent or executive director.

• Since there is no longer an Approve Access step at the agency, the IOwA role in EDIAM replaces the Admin role in MIDMS.

• IOwAs can now delegate their authority to authorize user access on behalf of their organization to an IOwA Proxy user role. The IOwA Proxy is NOT allowed to delegate.
How do users get access using EDIAM?

• Users get access to a secure application using EDIAM when the IOwA for their organization grants access to their user ID.

• There is no waiting period: as soon as the IOwA grants access to their user ID, they have that access.

• To grant access, the IOwA will need to know either their EDIAM user ID or the email address associated with their EDIAM user ID.

• Unlike MIDMS, there is no way to “request access” within the EDIAM system. Since the definition of Identified Official with Authority (IOwA) is the person responsible for assigning job duties, the IOwA (and their assigned IOwA Proxies, if applicable) is expected to know who needs access to State of Minnesota Education secure applications on behalf of their organization.

• If users do need to inform the IOwA that they need access to a secure application, they may use any form of communication appropriate for their organization (e.g. phone, email, helpdesk, etc.)
The IOwA launches the EDIAM Authorization System.
Each user of the EDIAM Authorization System must consent to communicate the Education Secured Website User Access Agreements and Acknowledgements to each person who they grant access to EDIAM-secured systems.
The IOwA can search for the user by either EDIAM User ID or Email Address. The IOwA must know the exact User ID or Email Address; no partial search is allowed.
The IOwA reviews the User ID, First Name, Last Name, and Email Address to verify that they have selected the correct user. If so, the IOwA selects the Add User Role action.

<table>
<thead>
<tr>
<th>Actions</th>
<th>User Id</th>
<th>First Name</th>
<th>Last Name</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add User Role</td>
<td>daviduser</td>
<td>David</td>
<td>Reeg</td>
<td><a href="mailto:david.reeg@state.mn.us">david.reeg@state.mn.us</a></td>
</tr>
</tbody>
</table>

(Exact User Id only search done for security reasons)
An individual who is IOwA for more than one organization must first select which organization on behalf of which they are granting access (also known as the “Authorizing Organization”).

<table>
<thead>
<tr>
<th>Selected</th>
<th>Organization Name</th>
<th>Formatted Id</th>
<th>State Organization Id</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>College and Career Success</td>
<td>0002-99</td>
<td>990000200000000</td>
</tr>
<tr>
<td></td>
<td>School Finance</td>
<td>0006-99</td>
<td>990000600000000</td>
</tr>
<tr>
<td></td>
<td>Compliance and Assistance</td>
<td>0010-99</td>
<td>990001000000000</td>
</tr>
<tr>
<td></td>
<td>MN.IT @ Education</td>
<td>0015-99</td>
<td>990001500000000</td>
</tr>
</tbody>
</table>

![Screenshot of EDIAM Authorization - Select Authorizing Organization page](image-url)
The IOwA selects which application to grant access to this user.
After selecting the application, the IOwA selects which application role to grant access to this user. Hovering the mouse over the role name will display the role description. The Authorize Role action completes the process.
To grant a user the **IOwA Proxy** role, the IOwA will select the EDIAM Authorization System application. The IOwA Proxy role has equivalent access to the IOwA and is useful for assigning one or more backup IOwA users.
When the Add User Role action is completed, EDIAM Authorization displays a list of authorized users. The IOwA can then add another user role to the same user or another user.
EDIAM Authorization sends an automated email notification to the user informing them of the user role(s) they have been granted.

The email notification provides the user with contact information for the Identified Official with Authority (IOwA) who granted the access.

Dear David Reeg,

The Identified Official with Authority David Reeg has granted you the following system security access:

Application: ComplianceDataTracking with User Role: Helpdesk User at Organization: Compliance and Assistance

You can view your security profile at the Minnesota Department of Education website page for Education Identity Access Management (EDIAM).

This is an automatically generated message, so please do not reply to this email. If you have any questions, contact the Identified Official with Authority David Reeg at david.reeg@state.mn.us.
Thank You!

David Reeg
MNIT Services partnering with Minnesota Dept. of Education
david.reeg@state.mn.us