MIDAS Account Creation
A step-by-step guide

Release: Oct. 31st, 2010

Getting Started
To activate your MIDAS account, go to a web browser and enter https://midas.odu.edu. Click on “Create MIDAS Account” in the menu on the left-hand side of the screen.

You have two options to create your MIDAS account. You can either use your “Leo Online” Credentials or the “Personal Information Validation”. If you are unsure or do not have your “Leo Online” information, then skip over “Leo Online Validation” and use the “Personal Information Validation” process to create you account.
Leo Online Validation
Enter your University ID (on your student or faculty/staff card) and PIN into the “Leo Online Validation” fields and then click on the “Leo Online Validation” button. If you do not know your University ID, then go to the “Leo Online” login page and follow the directions to retrieve it:
https://www.leoonline.odu.edu/plsql/web/twbkwbis.P_WWWLogin
When you do have the information, proceed with the “Leo Online Validation”.

NOTE:
If you do not know your Leo Online User ID or PIN, then you may complete the Personal Information form BELOW to validate your identity.

Personal Information Validation
You must provide the following Personal Information before you may activate your MIDAS Account.

- **First Name:**
- **Last Name:**
- **University ID/UNI:** Enter your “Leo Online User ID” or “UNI”.
- **Date of Birth:** Example 12/31/1970
- **Gender:** Male or Female

Click the appropriate radio button.
Personal Information Validation

Skip the Leo Online Validation and scroll down the page. You will see the following screen. Enter your personal information as instructed by gray boxes on the right-hand side of the screen. All fields are required.
Account requirements

Acceptable Usage Policy

Read the entire Acceptable Usage Policy (AUP). After reading the AUP select the “Accept” radio button and click “Submit”.

Acceptable Usage Policy

You Must Re-Sign This Policy Oct 28, 2011

Computer and network users are granted access to computing, networking, and information stored electronically contingent upon their prudent and responsible use. Access is granted to the individual and no individual can transfer or share access with others. Customers may not (1) use information or resources for any illegal or unauthorized purposes or act, i.e., to violate state or federal laws or any established policies and procedures if the University; (2) participate in any behavior that unreasonably interferes with the fair use of other customers or harms them in any way; (3) use resources or information for commercial purposes without prior authorization from the Vice President for Administration and Finance. (Note that these acceptable usage policies are in addition to policies established by the Commonwealth of Virginia and do not supersede those Commonwealth policies.)

Misuse of computing, networking, and information resources may result in severe consequences, including the loss of access to computing resources. (Please be aware that this loss of access could adversely affect the fulfillment of your University obligations.)

By accepting, I acknowledge understanding of the information contained above and agree to the following: (1) in any investigation of suspect misuse by the account owner, the University may inspect without prior notice (but with VP of Accounting authorization), the contents of files, voice mail, logs, and related compute-generated or stored material, such as printouts, and (2) customer computer files may be inspected occasionally by systems personnel when assessing system integrity or performing related resource management duties.

*You MUST scroll to the bottom of the AUP in order to Accept or Decline.
You MUST accept the AUP in order to continue.

DISCLAIMER: Failure to accept the Acceptable Usage Policy will result in denial of accounts or the disabling of existing accounts. Declining the AUP will disable any existing services and prevent new services from being activated.

Accept
Decline
Submit
**MIDAS PIN**

To make your account more secure, enter a 6-digit PIN number. Rules for the pin are in the gray box on the right-hand side of the screen. Click the “Set Pin” button.
Security Profile

The Security Profile is necessary to protect your privacy and the security of the network if you should forget your password. The setup consists of 3 steps.

In step 1 you choose a security token method. You have to choose at least one of them, but you can also choose multiple or all methods. Click the “Continue” button.
Step 2 requires you choose a verification method. You have 2 choices: a text-based method or a color-based method. Move your mouse pointer over the choice names to see examples. Click the “Continue” button to go on.

Depending on what you chose in step 2, the last step for the security profile is either the “Questions and Answers” profile or the “Color Grid Pattern” profile.
Questions and Answers profile
Please select 2 of the predefined questions and answer them. Make sure you select questions which you can answer in a unique fashion. Enter answers that you are able to recollect even months after the initial setup date. Click on “Submit Profile” when you’re finished.
Color Grid Pattern Profile

The Color Grid Pattern is intended for visually inclined people. Please follow the instructions on the page and click “Submit” when you’re done.
Training

You are required to take one or more training courses during account setup. The number of courses depends on your role within the university (faculty, staff or student). Please read carefully, click the “next” button to go to the next page. On the last page, click the “Accept” button.
Required MIDAS Training

<table>
<thead>
<tr>
<th>2009 Midas General Security Training</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Training Awareness for All Users, Page 9 of 9</td>
</tr>
</tbody>
</table>

**Certification of Training**

Congratulations!

You have completed the 2009 Information Technology Security Awareness Training. Depending on your role and access requirements, additional training may be required and will be presented next.

**Accept or Decline:**

Clicking on the 'Accept' button indicates that you certify that you have read and understand the materials presented in this training and that you accept the responsibilities associated with using these assets. Continued use of the IT assets of Old Dominion University requires this acceptance.

Clicking on the 'Decline' button indicates that you have not read, do not understand and/or do not accept the responsibilities presented in this training material. You will then NOT qualify for continued use of these IT assets.
Password

The final step in your account setup is the setting of a password. The password must follow certain rules to be valid as a MIDAS password. These rules ensure the security of your password and are listed in the grey box on the right-hand side of your screen. You will see a progress bar that indicates if all the password rules are complied with. The rules themselves change style once you comply with them, so you can adapt your new password accordingly. Click the “Change Password” button.
**Account Information**

Your account is set up. On the top of the page a message will appear that displays your new Midas ID. Please make sure to **write down your Midas ID**!

To log out of MIDAS, click on “Log out of MIDAS” on the left side of the screen.

Please call the Help Desk at (757) 683-3192 or email occshelp@odu.edu if you have any additional problems.