AccessVUMC

Identity Management tool

User Guide

Change a Password
Set your Display Name
Reset a Forgotten Password

VANDERBILT UNIVERSITY
MEDICAL CENTER

Information Technology

AccessVUMC Utilization Requirements

Please note:

To utilize the AccessVUMC Identity Management tool, enrollment in Multi-Factor Authentication is required. This extra layer of security ensures that your personal identifiable information (PII) is protected.

If you are not already enrolled, visit the Enterprise Cybersecurity website at: https://www.vumc.org/enterprisecybersecurity/multi-factor-authentication-mfa

AccessVUMC – What's new?

- **AccessVUMC is the new Identity Access Management tool for our workforce**.
  - Check out the new AccessVUMC homepage
- **Enrollment in Multi-Factor Authentication is a requirement** to protect and manage your VUMC ID information.
  - See the MFA sign on experience
- **All current usernames and passwords will remain the same**, however usernames are now called VUMC IDs.
- **Managing your VUMC account looks and feels different** on the AccessVUMC dashboard.
  - How to Change your Password
  - How to Set your Display Name
  - Forget your password? See how to Reset your Password

Visit the AccessVUMC Identity Management Project home page for more information.

AccessVUMC – What's the same?

- **Most processes are the same** within AccessVUMC, they just look and feel different on the new dashboard
  - Claiming a new account is the same
  - Claiming an invitation is the same
  - Claiming a MAC Account is the same
  - Entering Personal Identifiable Information (PII) is the same
  - Claiming a Resource Account is the same
  - Claiming a Test Account is the same
- **Your username and password will remain the same; however, they will now be called a VUMC ID.**

Visit the AccessVUMC Identity Management Project home page for more information.

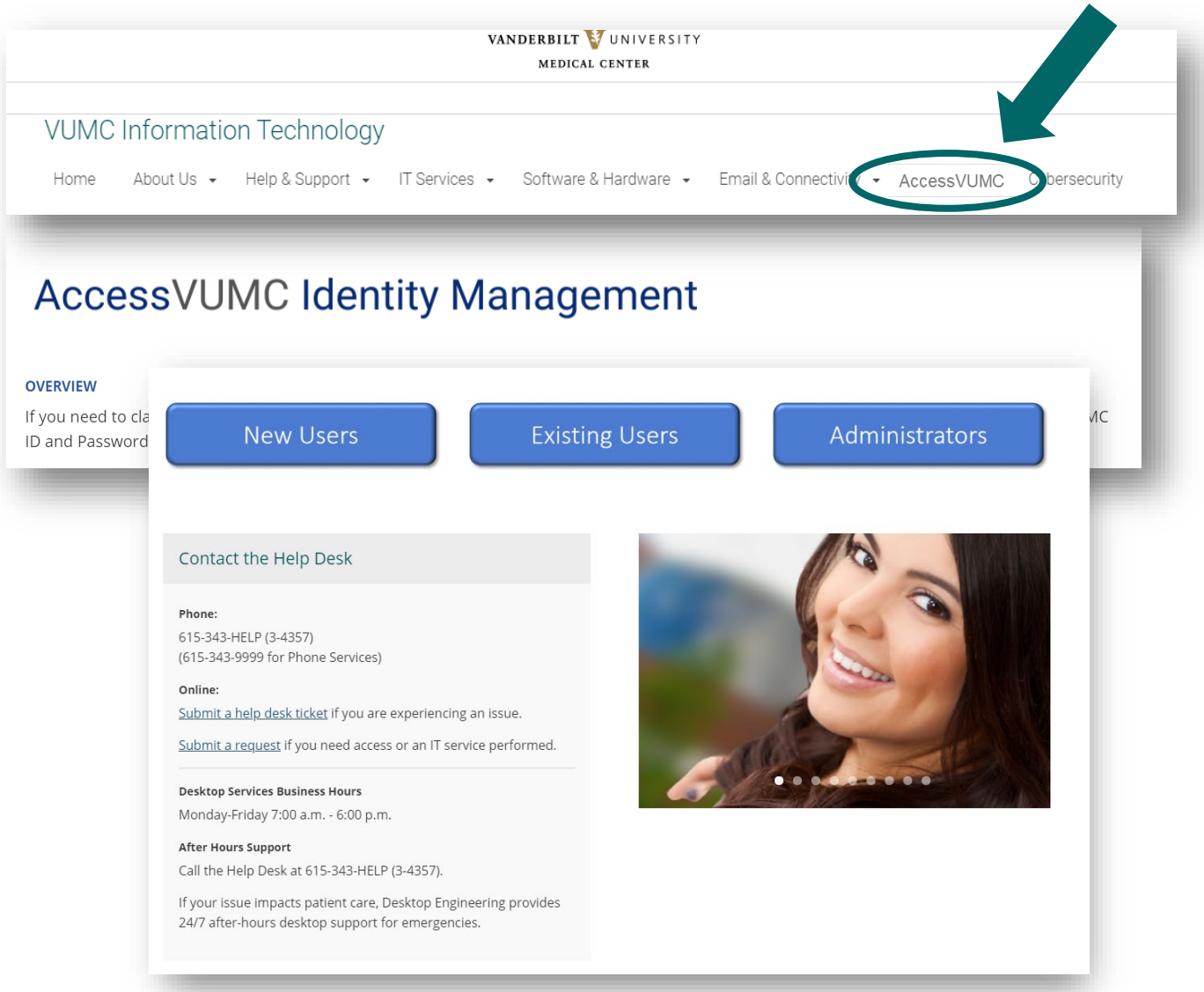
The new AccessVUMC home page

If you have a valid VUMC ID and password, and are enrolled in Multi-Factor Authentication, you can use AccessVUMC to manage your identity.

Find the new AccessVUMC home page at:

https://www.vumc.org/it/accessvumc.

Return to “What’s New” Menu



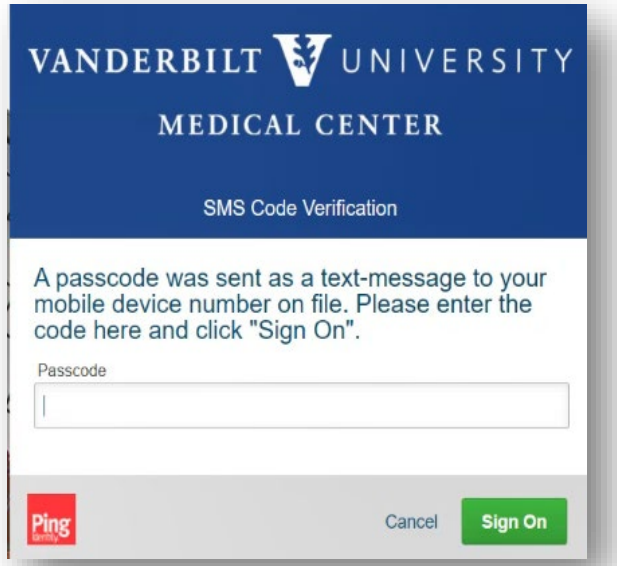
Sign-On using Multi-Factor Authentication

When you sign on, you will be prompted to authenticate using Multi-Factor Authentication. If you haven't enrolled already, visit www.vumc.org/enterprisecybersecurity/mfa.

NOTE: Your MFA sign on experience will vary based upon your MFA enrollment status (e.g. token, SMS texting, etc.).

MFA Sign on for SMS Text users

MFA Sign on for Token users



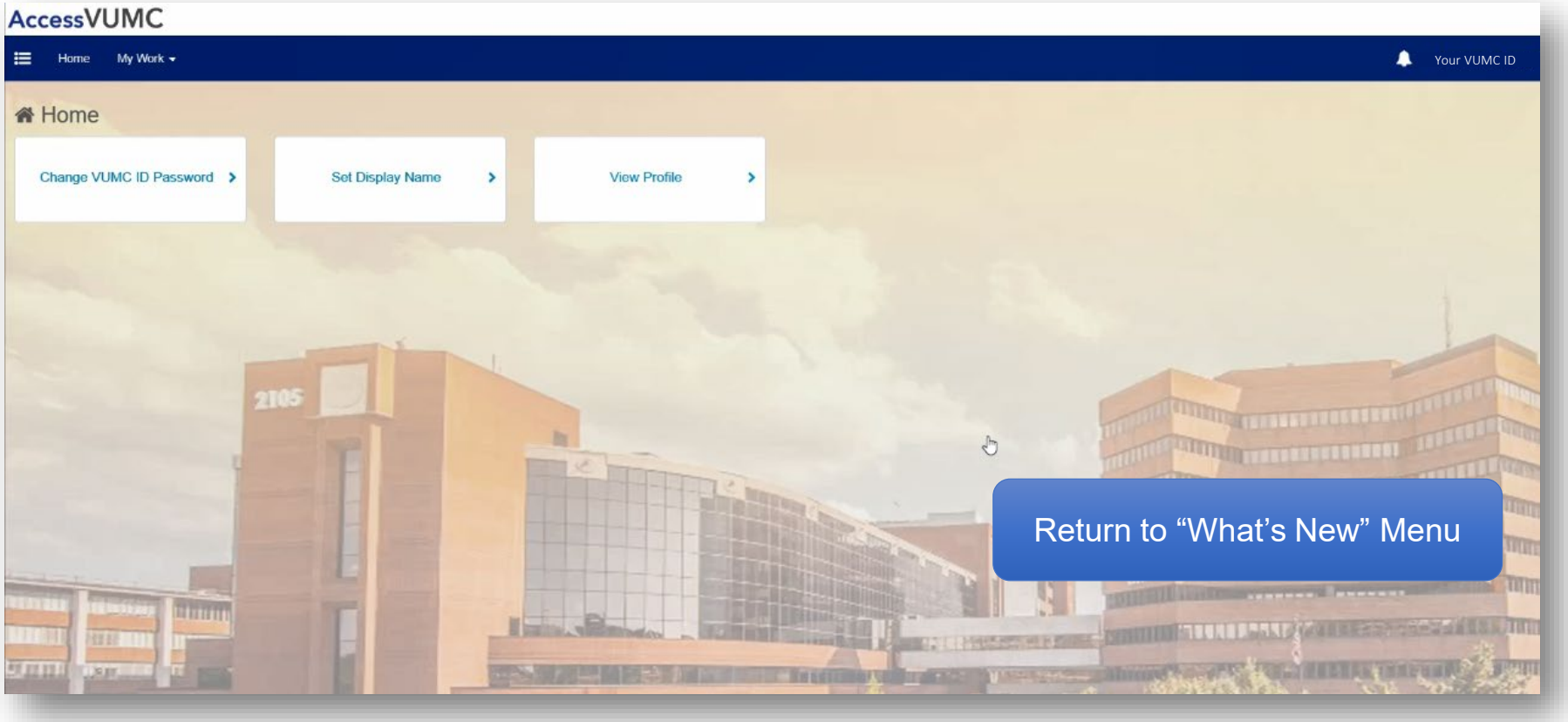
Return to "What's New" Menu

AccessVUMC Identity Management

The new AccessVUMC Identity Management dashboard

Once you authenticate, the new AccessVUMC dashboard will appear. From here you can:

- Change your VUMC ID Password
- Set your Display Name
- View Your Profile
- Click on the ☰ menu button to access other options



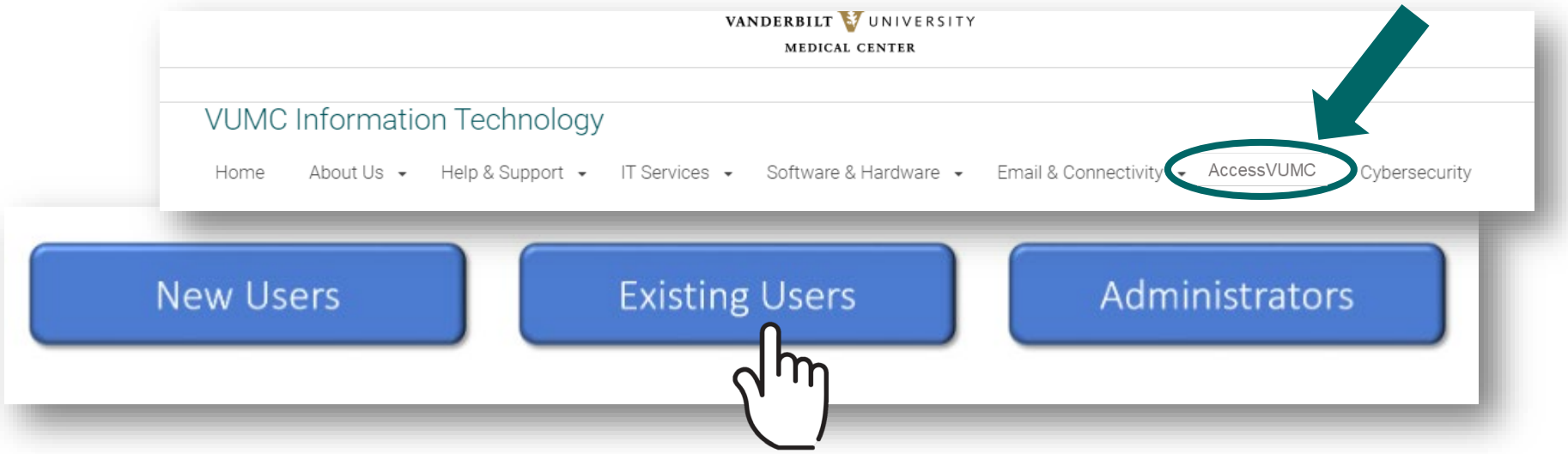
AccessVUMC Identity Management Tool
How to Change a Password

Return to “What’s New” Menu

Change your Password

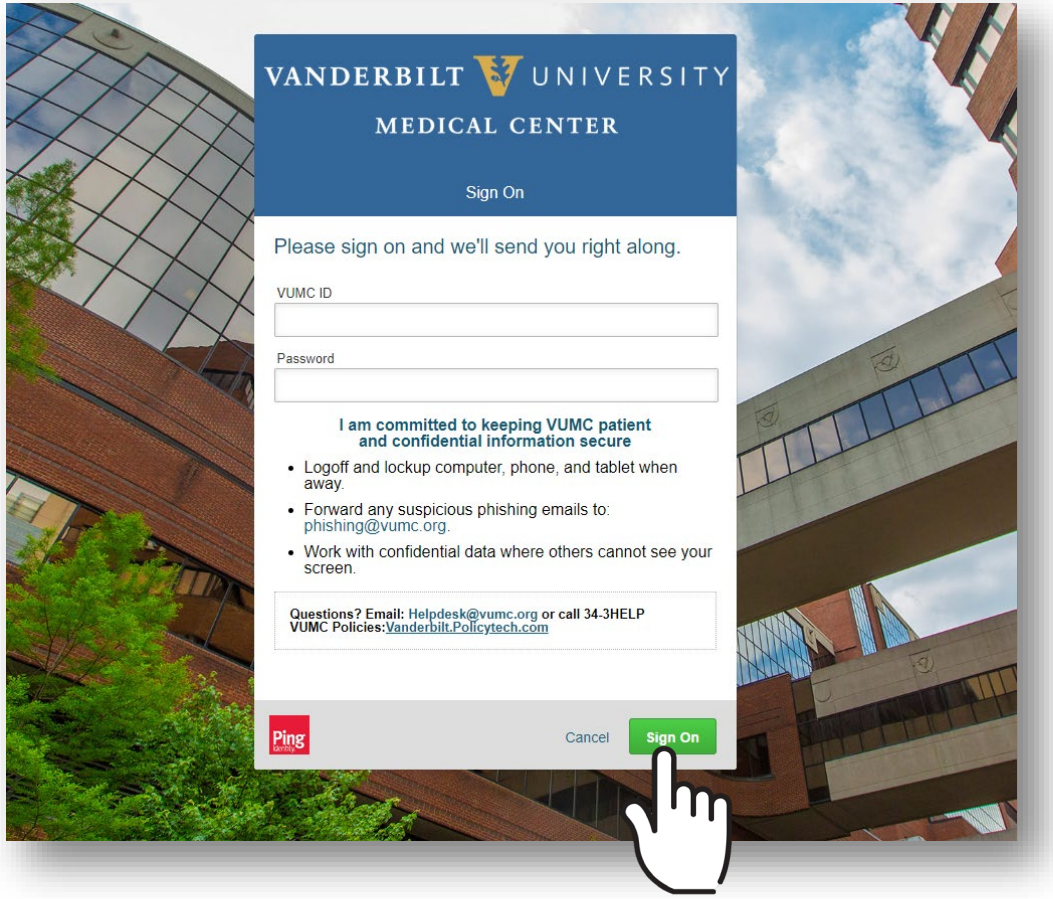
Users with a valid VUMC ID **AND** enrolled in Multi-Factor Authentication (MFA) can use AccessVUMC to change/reset a password.

- Click **Existing Users** from the AccessVUMC home page https://www.vumc.org/it/accessvumc.



Change your Password

- From the AccessVUMC home page, you will be prompted to authenticate using your VUMC ID and password.
- Click **Sign On**.



Change your Password

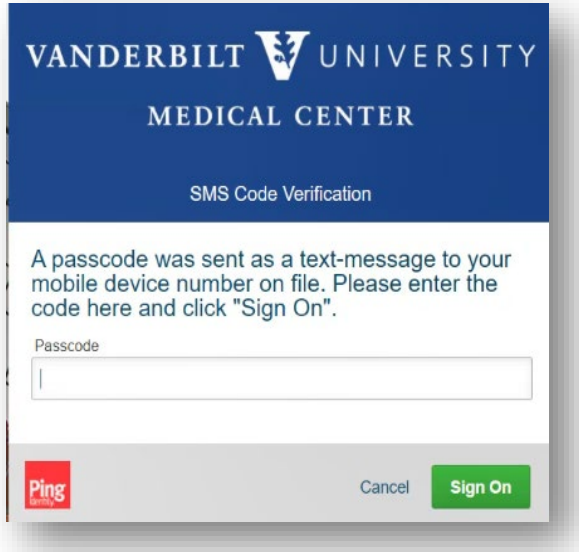
- You will then be prompted to enter a Multi-Factor Authentication passcode.

NOTE: Your MFA sign on experience will vary based upon your MFA enrollment status (e.g. token, SMS texting, etc.).

- Click **Sign On** once your have entered your passcode.

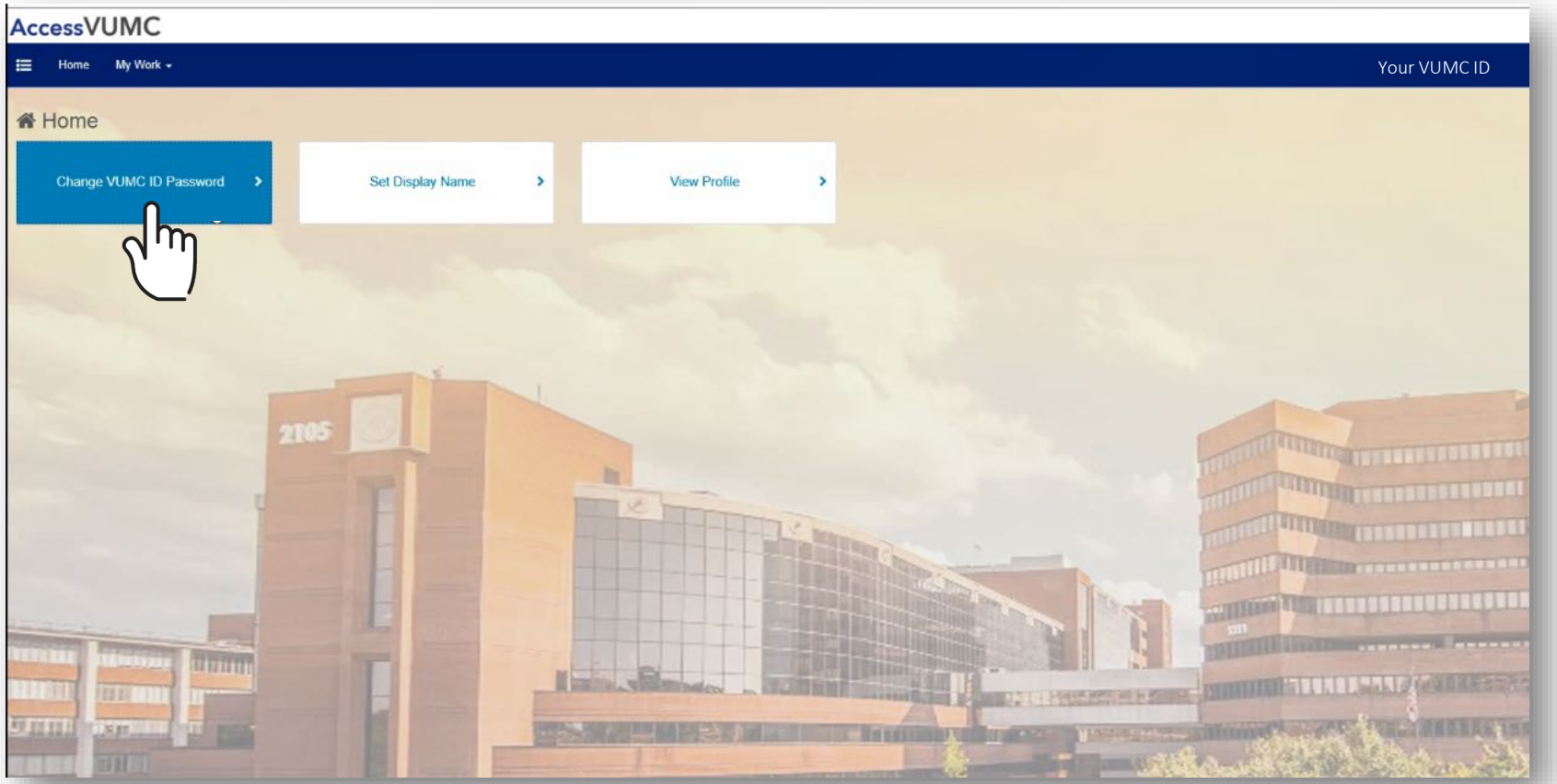
MFA Sign on for SMS Text users

MFA Sign on for Token users



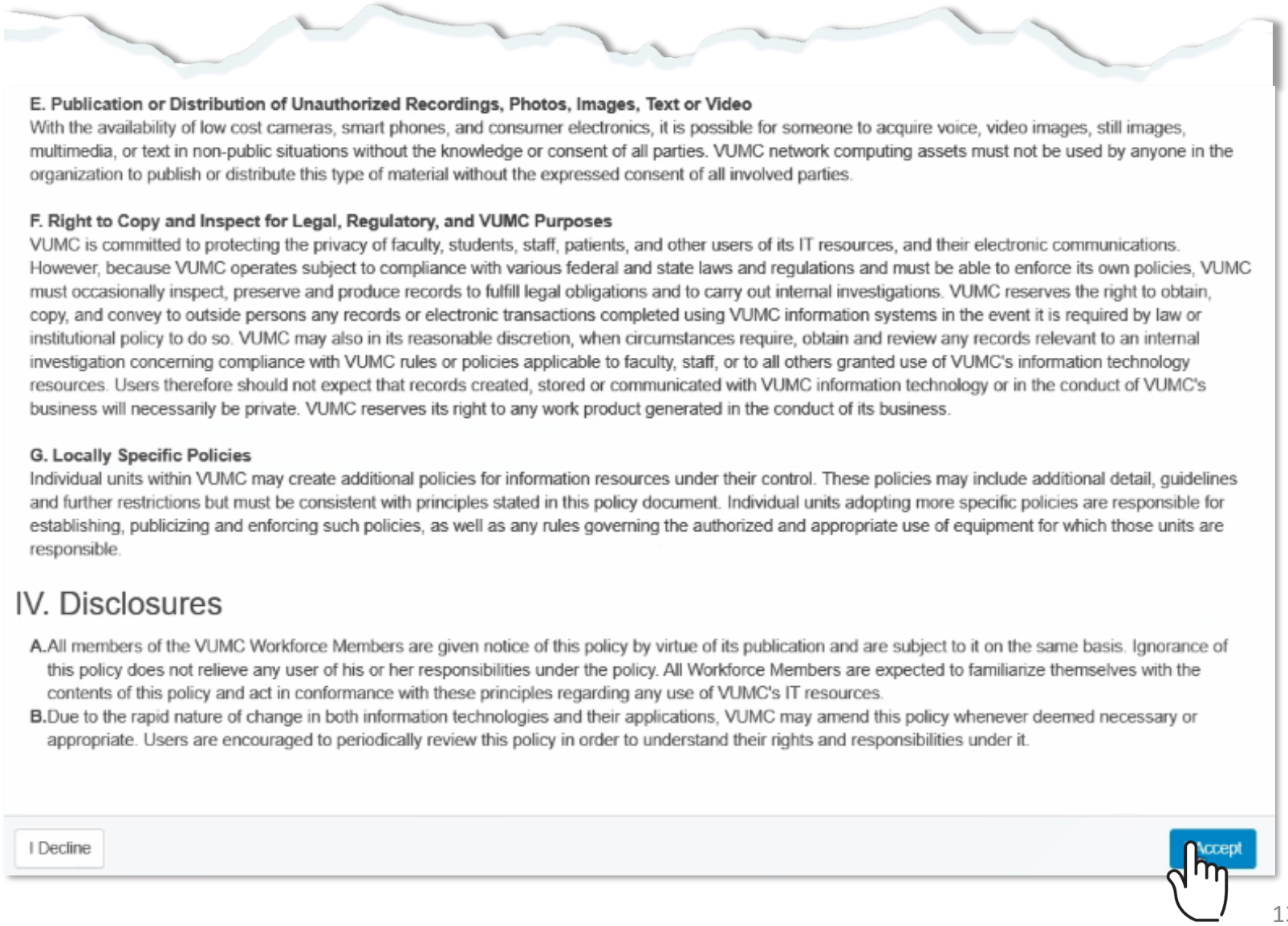
Change your Password

Click the **Change VUMC ID Password** button from the AccessVUMC dashboard.



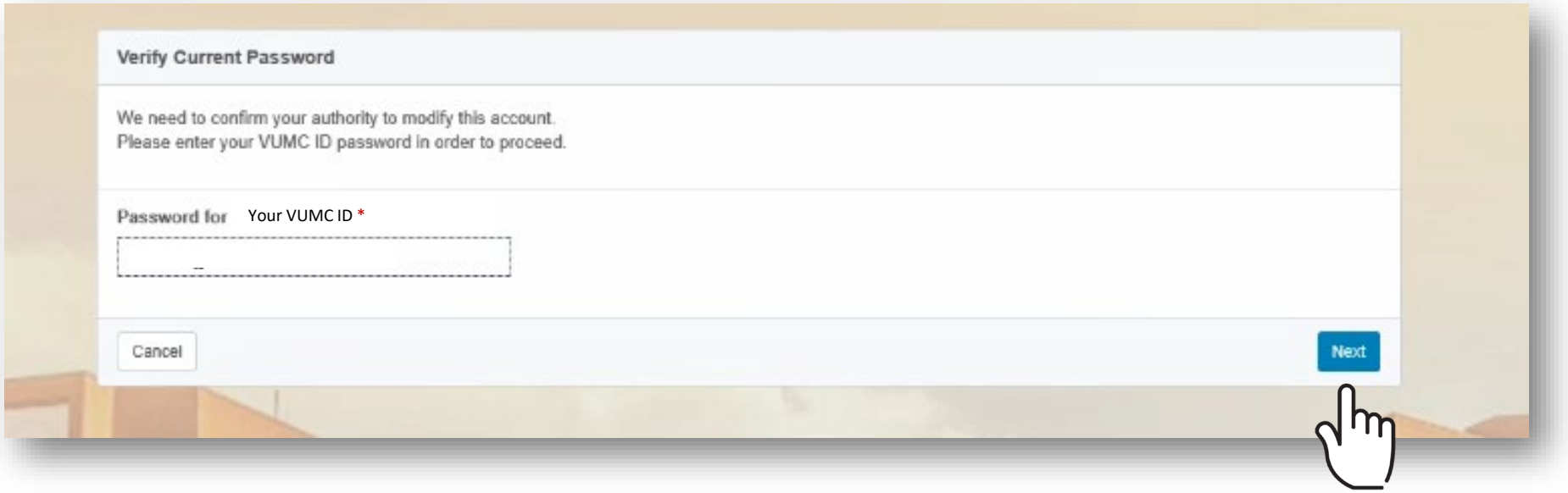
Change your Password

Click **Accept** once you have read the VUMC Acceptable Use Policy regarding your computer privileges and responsibilities.



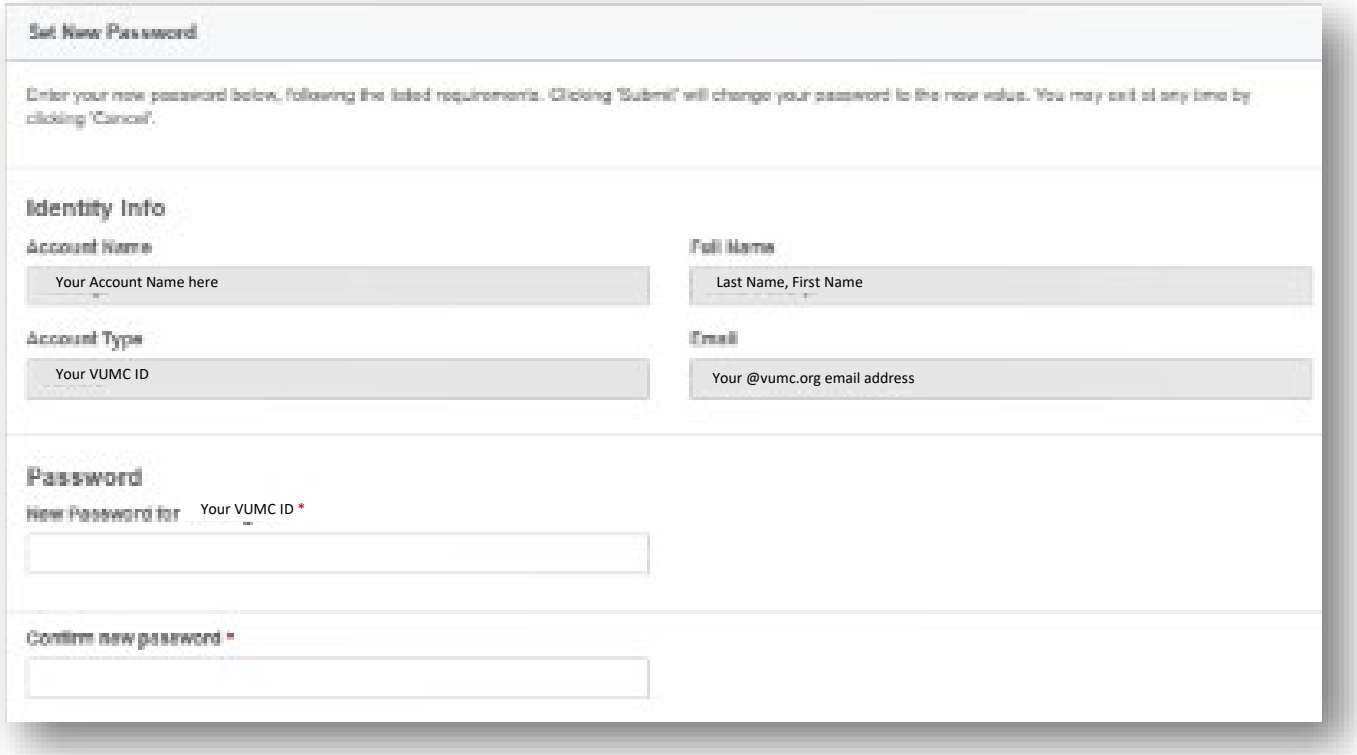
Change your Password

- Verify your current password.
- Click **Next**.



Change your Password

- Enter and confirm your **NEW** password.
- Click **Submit**.



Keep these 3 password basics in mind when you create your VUMC Account password.

1. You cannot reuse your last 10 passwords
2. Passwords MUST CONTAIN:
   - At most 16 characters
   - At least 1 lowercase letter
   - At least 8 characters
   - At least 3 character types
   - At least 1 number
   - At least 1 uppercase letter
3. Passwords CANNOT CONTAIN your:
   - Email address
   - Account last name
   - Display name
   - Account names in reverse

Change your Password

- You will receive a confirmation screen that your password was successfully re-authenticated.
- You will also receive an email that your password was changed.
- Click **OK**.

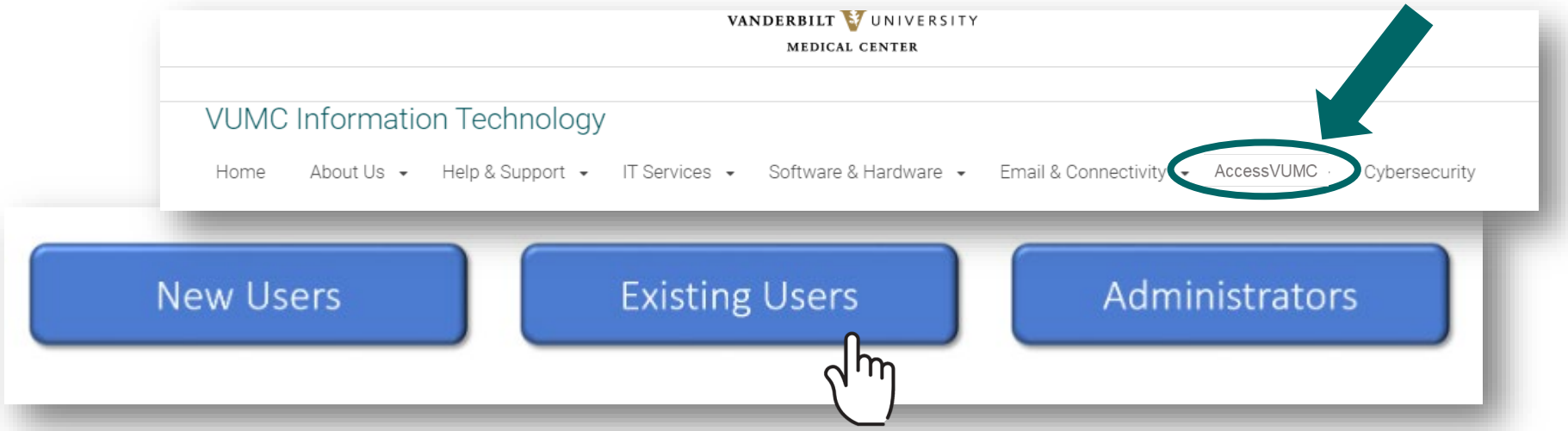
AccessVUMC Identity Management Tool
How to Set a Display Name

Return to “What’s New” Menu

Set your Display Name

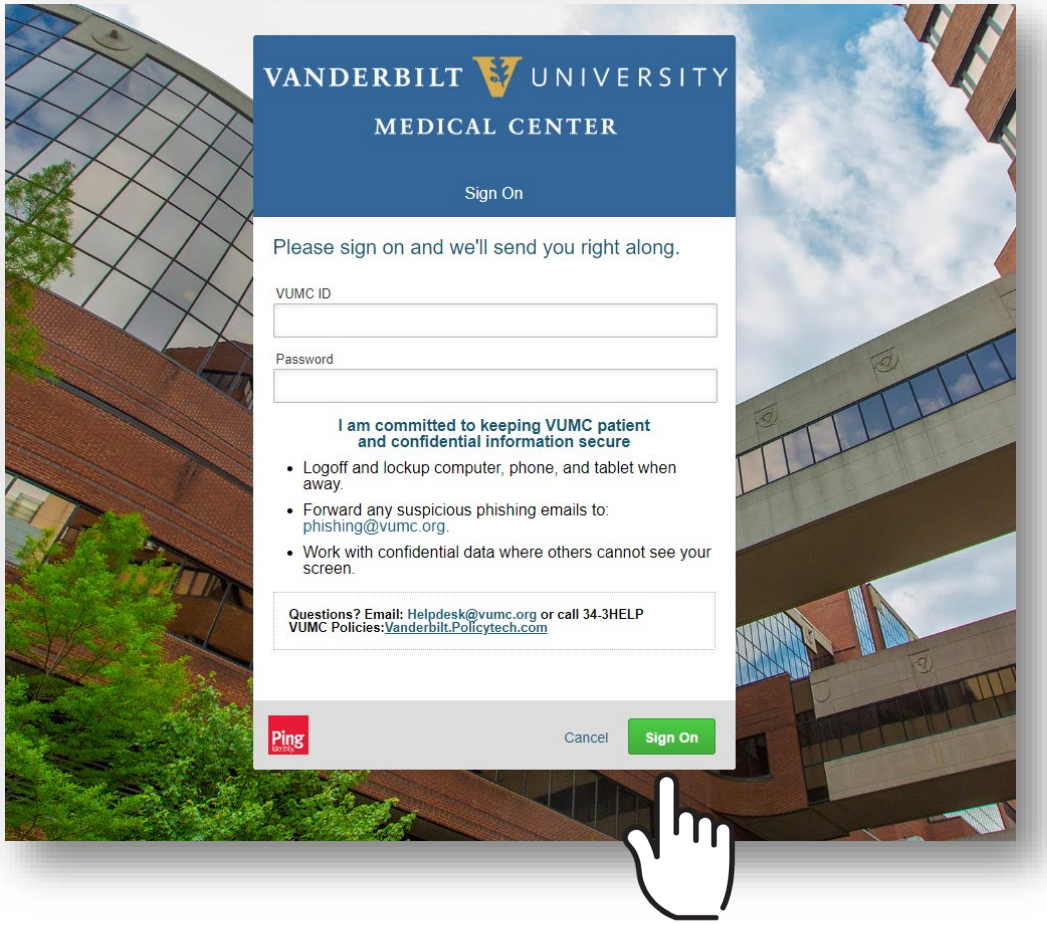
VUMC employees enrolled in multi-factor authentication AND with a valid VUMC ID can use AccessVUMC to Set a Display Name.

- Click **Existing Users** from the AccessVUMC website https://www.vumc.org/it/accessvumc.



Set your Display Name

From the AccessVUMC homepage, you will need to authenticate using your VUMC ID and password and **Sign On**.



Set your Display Name

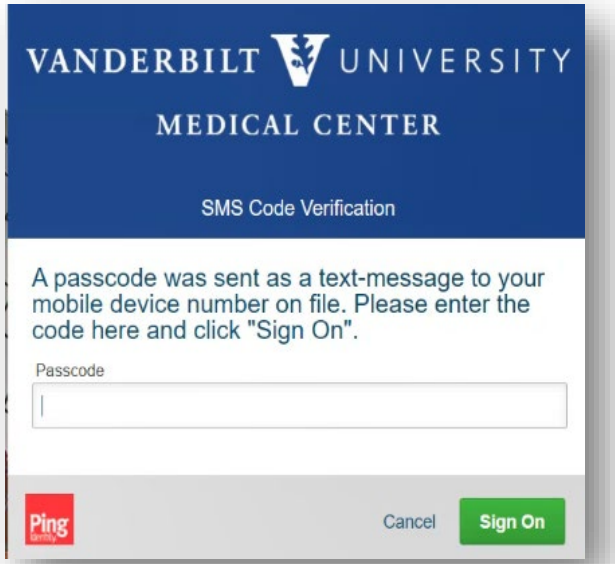
- You will then be prompted to enter a Multi-Factor Authentication passcode.

NOTE: Your MFA sign on experience will vary based upon your MFA enrollment status (e.g. token, SMS texting, etc.).

- Click **Sign On**.

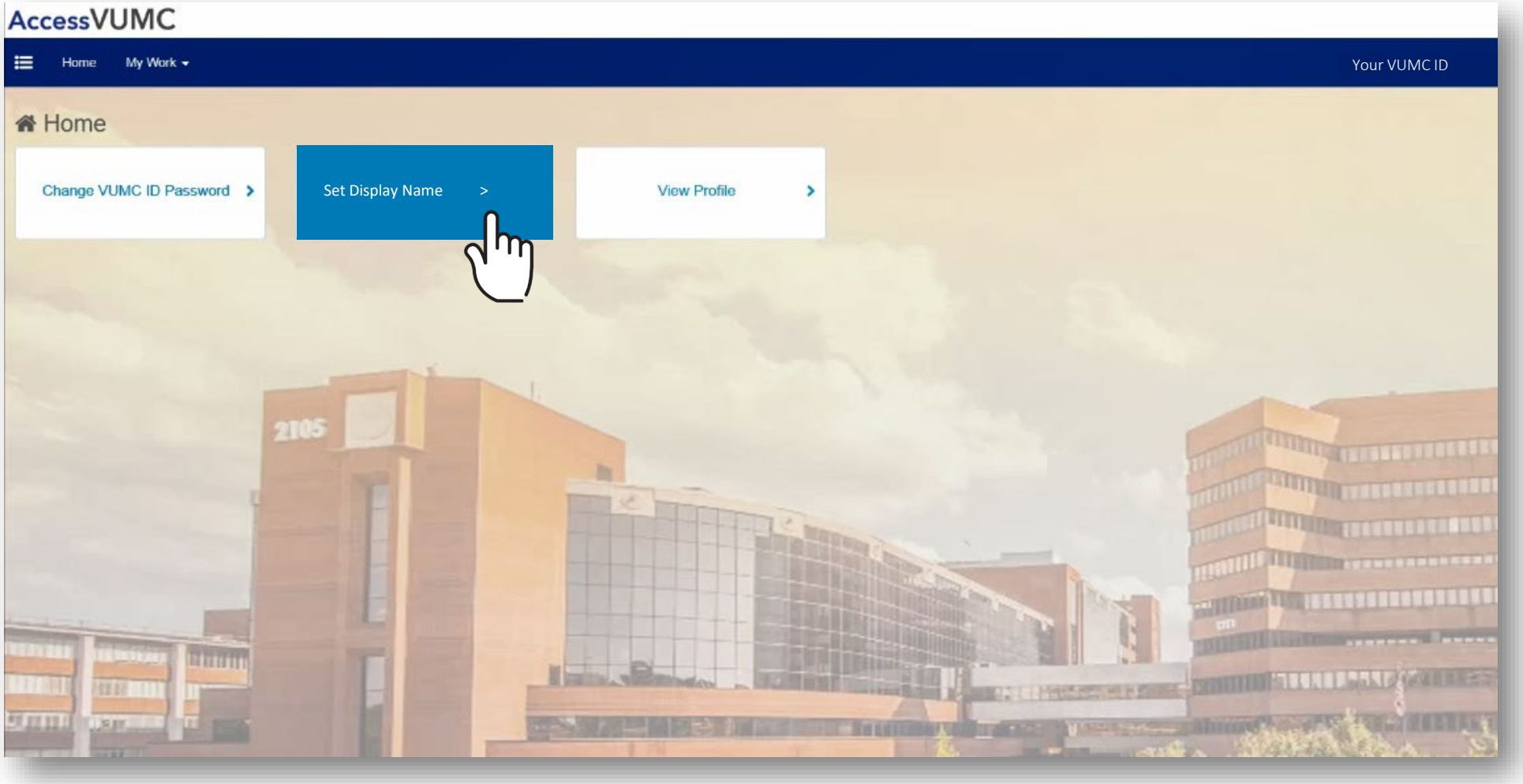
MFA Sign on for SMS Text users

MFA Sign on for Token users



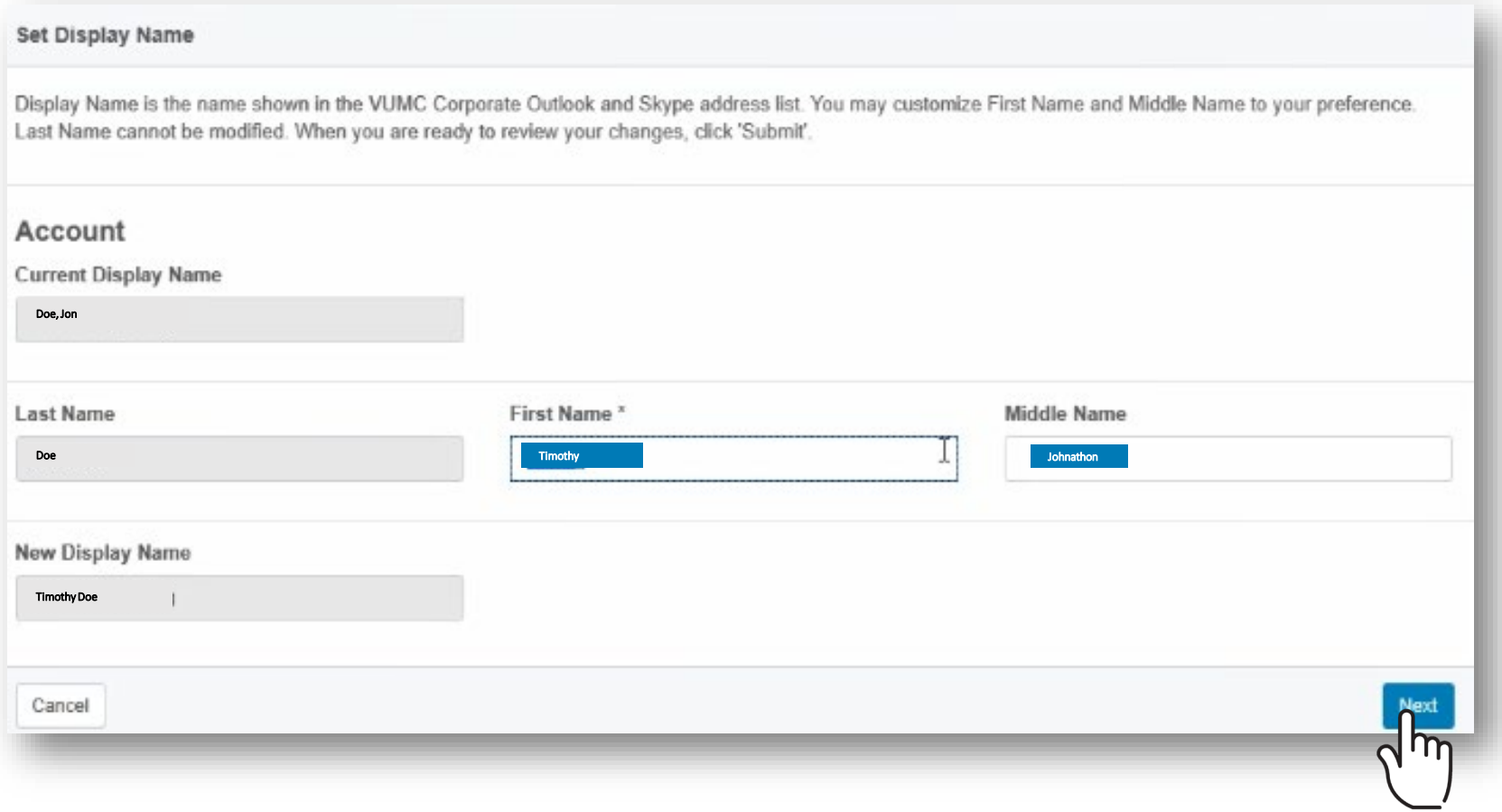
Set your Display Name

Click **Set Display Name** from your AccessVUMC Dashboard.



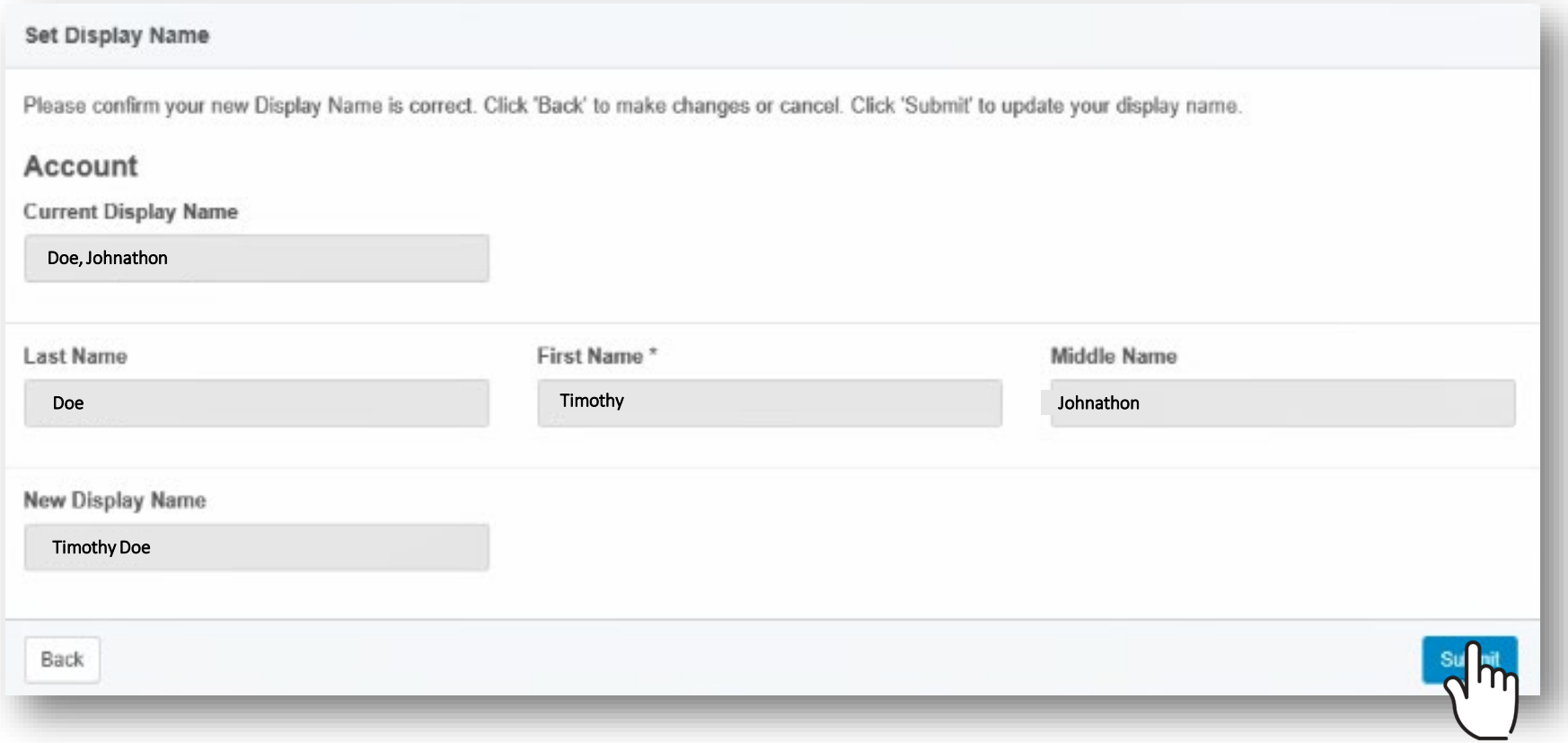
Set your Display Name

- The Account's **Current Display Name, Last Name, First Name and Middle Name** will automatically appear.
- Enter the **New Display Name**.
- Click **Next**.



Set your Display Name

- Confirm the new display name on your account.
- Click **Submit**.



AccessVUMC Identity Management Tool
How to reset a forgotten password

Forgot your password? Select your status:

1. VUMC employees enrolled in Multi-Factor Authentication
2. Active VUMC ID holders enrolled in Multi-Factor Authentication
3. VUMC employees or active VUMC ID holders not enrolled in Multi-Factor Authentication

Return to “What’s New” Menu

Reset a Password

For VUMC EMPLOYEES enrolled in Multi-Factor Authentication

AccessVUMC Identity Management

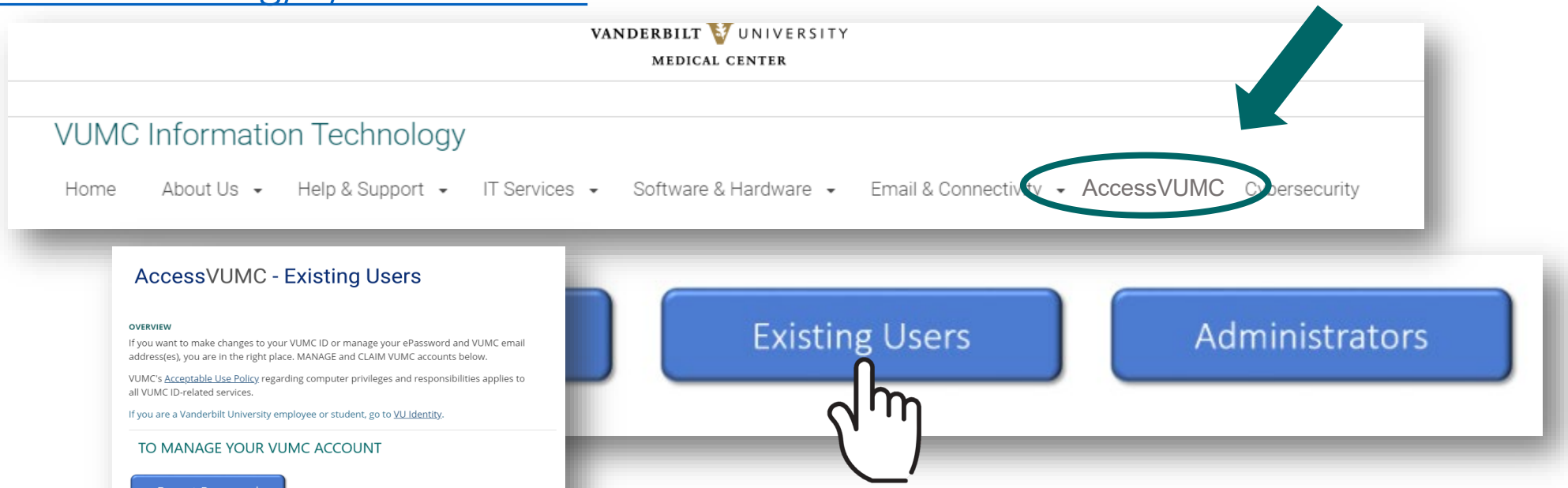
Return to “Reset Password” Menu

Reset a Password

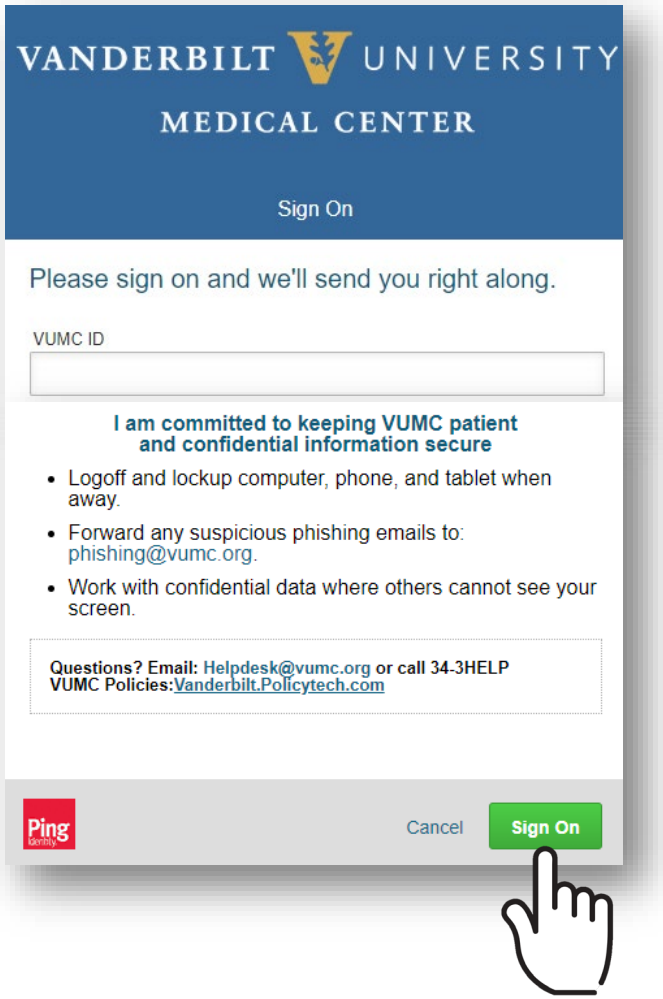
For VUMC EMPLOYEES enrolled in Multi-Factor Authentication

VUMC employees enrolled in Multi-Factor Authentication AND with a valid VUMC ID can use AccessVUMC to Reset a Password.

Click **Existing Users** and **Forgot Password** from the AccessVUMC home page. https://www.vumc.org/it/accessvumc.



- From the AccessVUMC home page, enter your VUMC ID.
- Click **Sign On**.



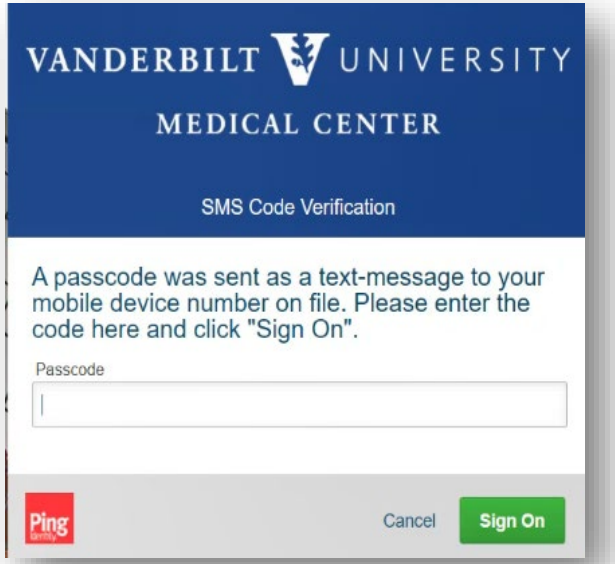
- You will then be prompted to enter a Multi-Factor Authentication passcode.

NOTE: Your MFA sign on experience will vary based upon your MFA enrollment status (e.g. token, SMS texting, etc.).

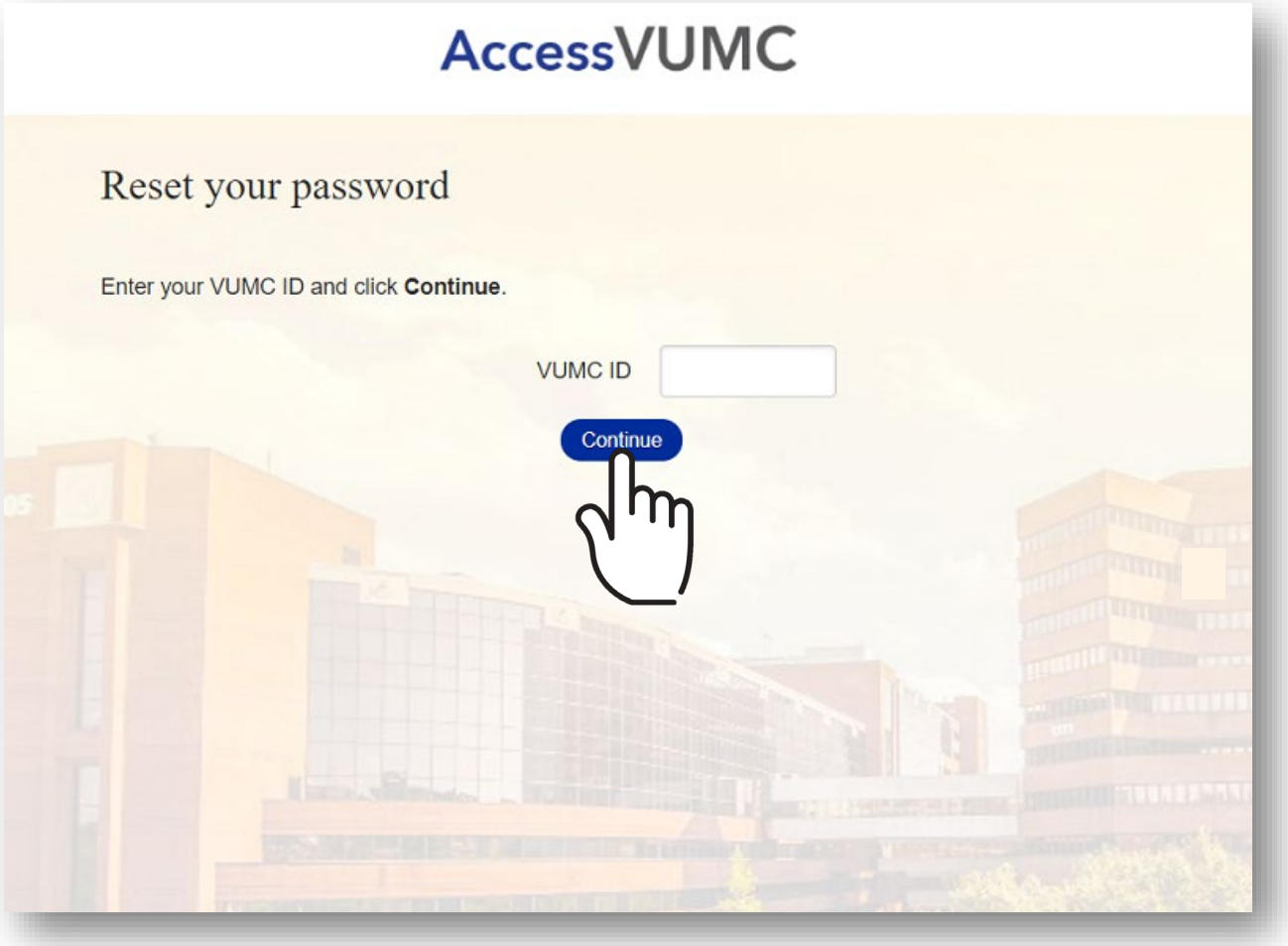
- Click **Sign On**.

MFA Sign on for SMS Text users

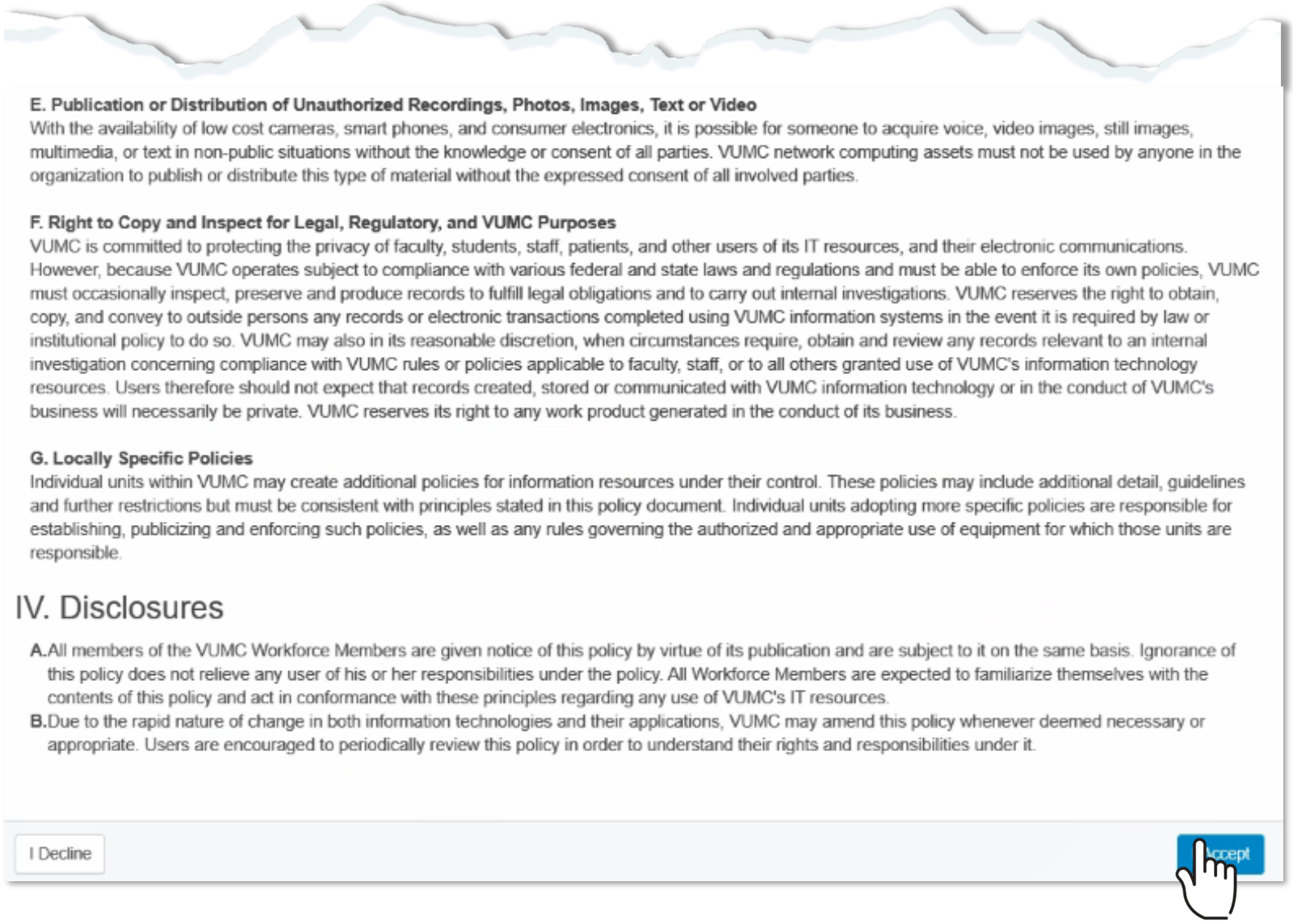
MFA Sign on for Token users



- Confirm your identity by entering your VUMC ID again.
- Click **Continue**.



Click **Accept** once you have read the VUMC Acceptable Use Policy regarding your computer privileges and responsibilities.



E. Publication or Distribution of Unauthorized Recordings, Photos, Images, Text or Video
With the availability of low cost cameras, smart phones, and consumer electronics, it is possible for someone to acquire voice, video images, still images, multimedia, or text in non-public situations without the knowledge or consent of all parties. VUMC network computing assets must not be used by anyone in the organization to publish or distribute this type of material without the expressed consent of all involved parties.

F. Right to Copy and Inspect for Legal, Regulatory, and VUMC Purposes
VUMC is committed to protecting the privacy of faculty, students, staff, patients, and other users of its IT resources, and their electronic communications. However, because VUMC operates subject to compliance with various federal and state laws and regulations and must be able to enforce its own policies, VUMC must occasionally inspect, preserve and produce records to fulfill legal obligations and to carry out internal investigations. VUMC reserves the right to obtain, copy, and convey to outside persons any records or electronic transactions completed using VUMC information systems in the event it is required by law or institutional policy to do so. VUMC may also in its reasonable discretion, when circumstances require, obtain and review any records relevant to an internal investigation concerning compliance with VUMC rules or policies applicable to faculty, staff, or to all others granted use of VUMC's information technology resources. Users therefore should not expect that records created, stored or communicated with VUMC information technology or in the conduct of VUMC's business will necessarily be private. VUMC reserves its right to any work product generated in the conduct of its business.

G. Locally Specific Policies
Individual units within VUMC may create additional policies for information resources under their control. These policies may include additional detail, guidelines and further restrictions but must be consistent with principles stated in this policy document. Individual units adopting more specific policies are responsible for establishing, publicizing and enforcing such policies, as well as any rules governing the authorized and appropriate use of equipment for which those units are responsible.

IV. Disclosures

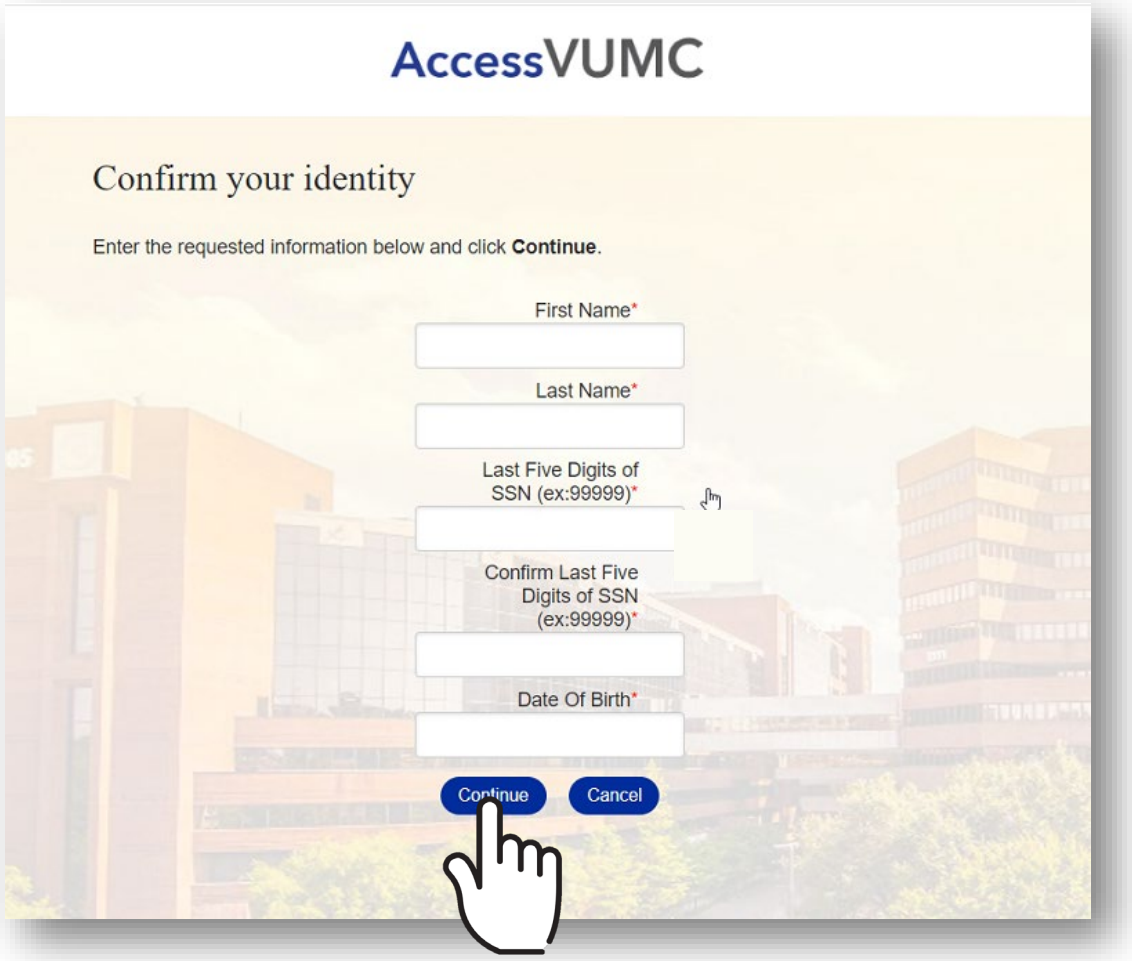
A. All members of the VUMC Workforce Members are given notice of this policy by virtue of its publication and are subject to it on the same basis. Ignorance of this policy does not relieve any user of his or her responsibilities under the policy. All Workforce Members are expected to familiarize themselves with the contents of this policy and act in conformance with these principles regarding any use of VUMC's IT resources.

B. Due to the rapid nature of change in both information technologies and their applications, VUMC may amend this policy whenever deemed necessary or appropriate. Users are encouraged to periodically review this policy in order to understand their rights and responsibilities under it.

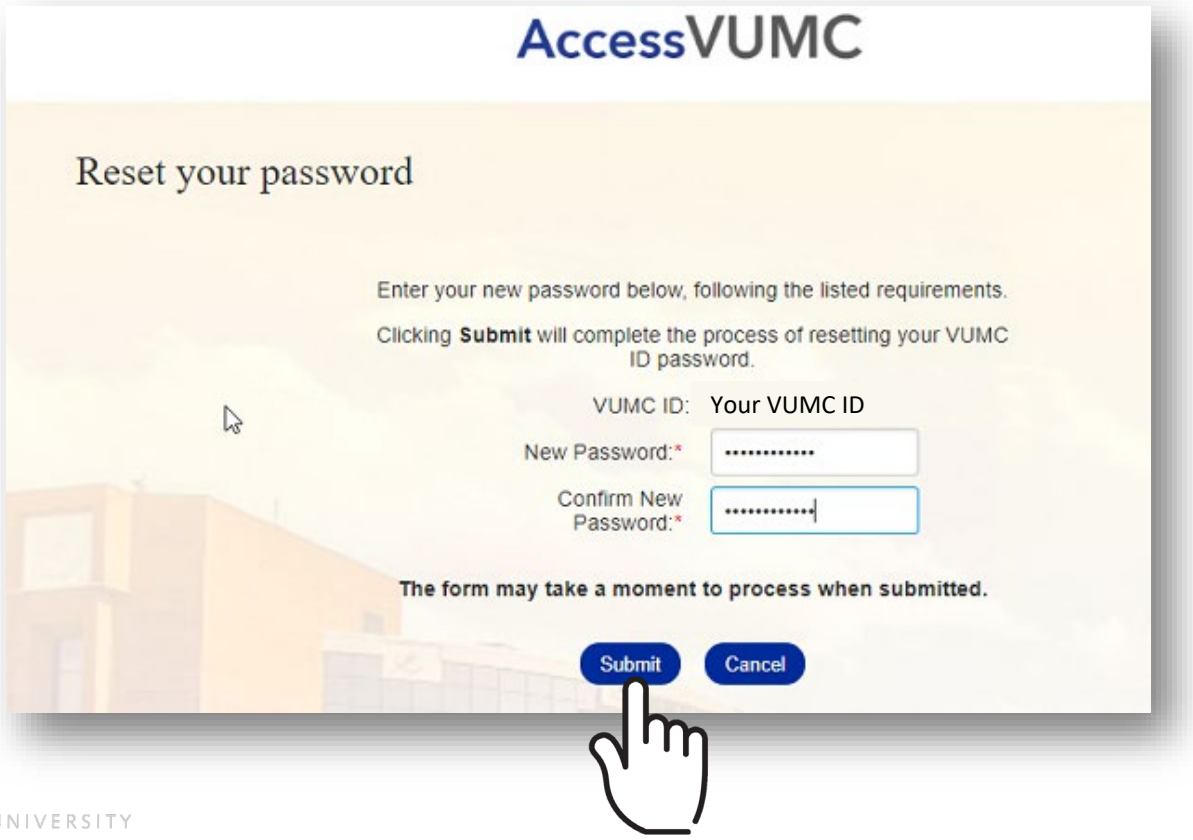
I Decline

Accept

- Confirm your identity by entering your personal identifiable information (PII).
- Click **Continue**.



- Enter your new password and confirm.
- Click **Submit**.



Keep these 3 password basics in mind when you create your VUMC Account password.

1. You cannot reuse your last 10 passwords
2. Passwords MUST CONTAIN:
   - At most 16 characters
   - At least 1 lowercase letter
   - At least 8 characters
   - At least 3 character types
   - At least 1 number
   - At least 1 uppercase letter
3. Passwords CANNOT CONTAIN your:
   - Email address
   - Account last name
   - Display name
   - Account names in reverse

- You will receive a confirmation screen that your password was successfully re-authenticated.
- You will also receive an email that your password was changed.
- Click **Finish**.

Reset a Password

For ACTIVE VUMC ID holders (not employees) enrolled in Multi-Factor Authentication

AccessVUMC Identity Management

Return to “Reset Password” Menu

Reset a Password

For ACTIVE VUMC ID HOLDERS enrolled in Multi-Factor Authentication

Active VUMC ID holders who have forgotten their password and are enrolled in Multi-Factor Authentication can use AccessVUMC to reauthenticate.

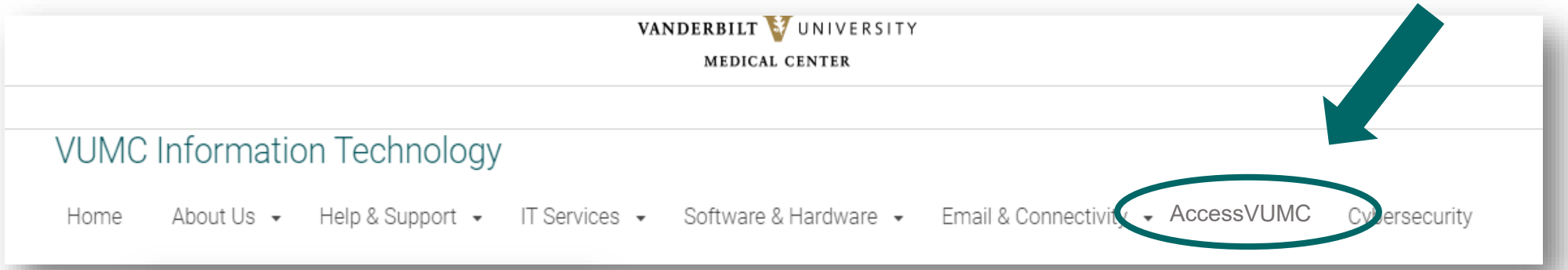
Please take the following steps to reset your password:

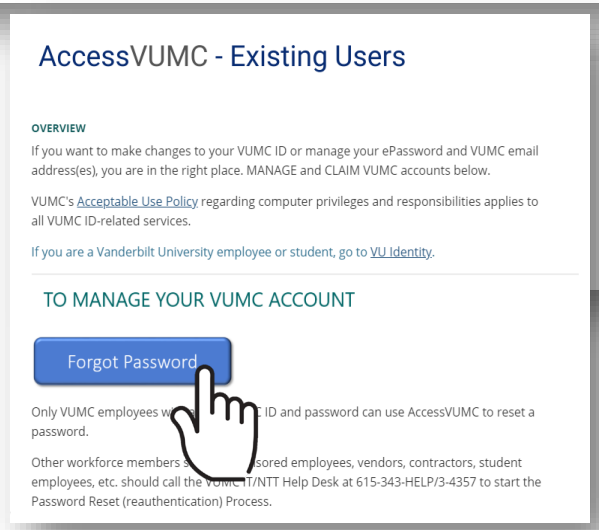
1. Contact the VUMC IT/NTT Help Desk at 615-343-HELP/3-4357 to start the Password Reset (reauthentication) Process.

2. When you receive your temporary login passcode, take the steps provided in the following slides.

Active VUMC ID holders include workforce members who are sponsored by departments including contractors, vendors, student employees, etc.

- After you have received your temporary MFA passcode, login to AccessVUMC at https://www.vumc.org/it/accessvumc.
- Click **Existing Users** and **Forgot Password**.

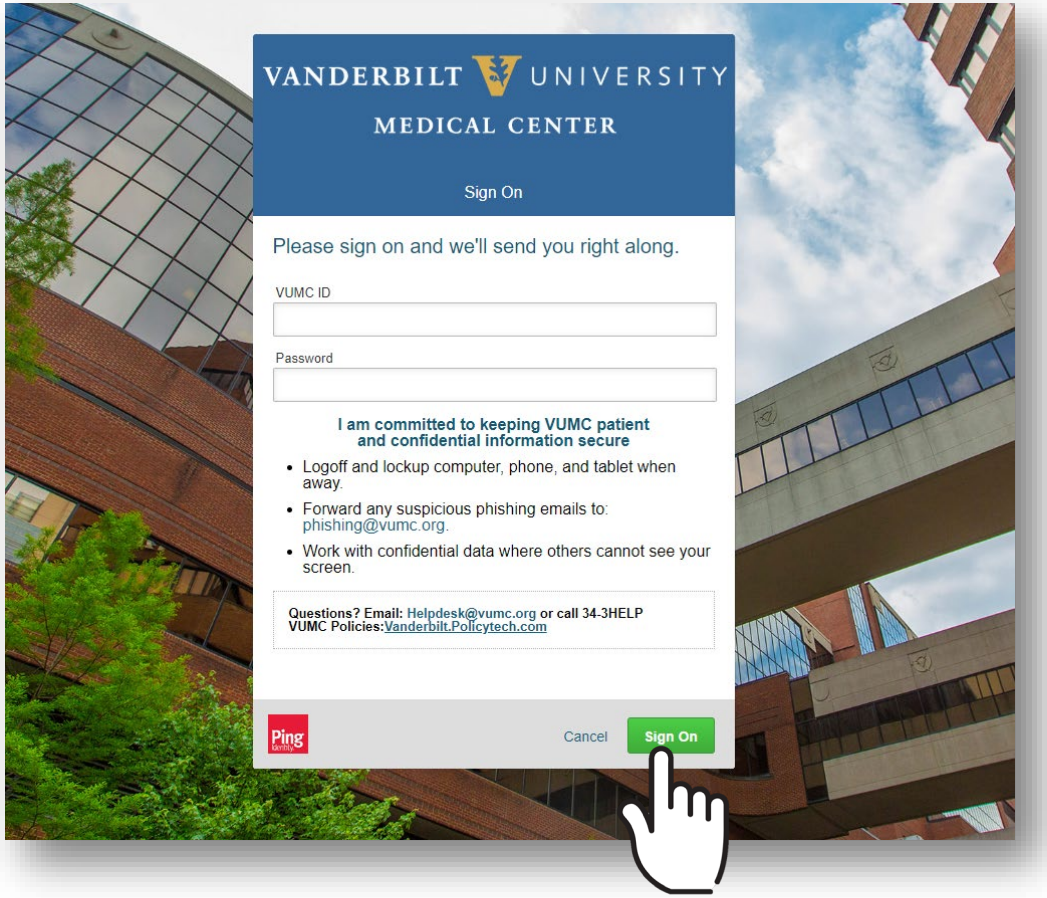




Reset a Password

For ACTIVE VUMC ID HOLDERS enrolled in Multi-Factor Authentication

- From the AccessVUMC homepage, you will need to authenticate.
- Use your VUMC ID and the temporary passcode you received from the Help Desk.
- Click **Sign On**.

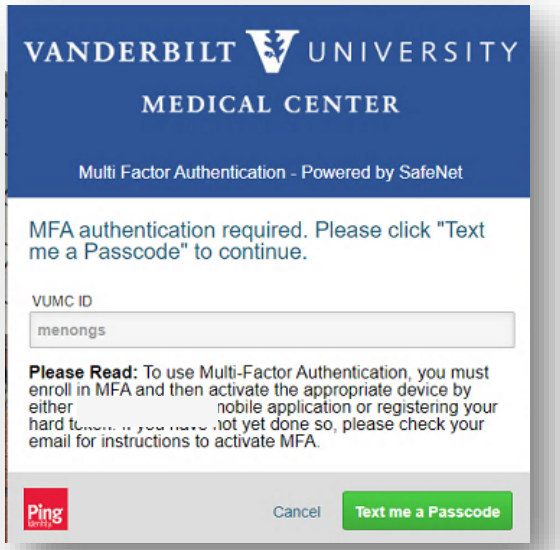


- You will then be prompted to enter a Multi-Factor Authentication passcode.

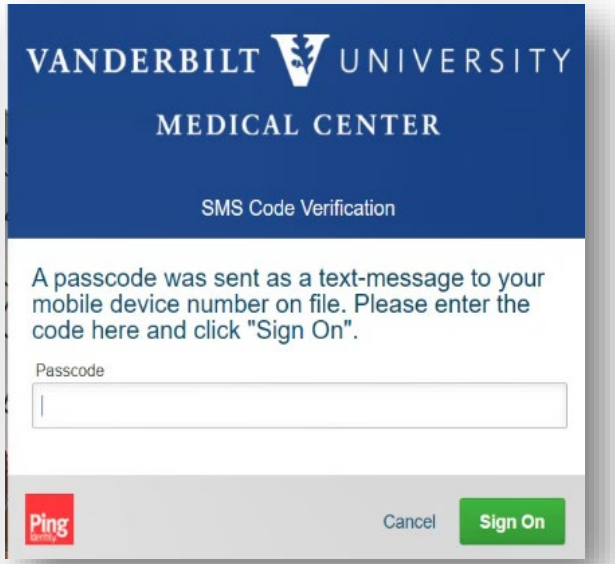
NOTE: Your MFA sign on experience will vary based upon your MFA enrollment status (e.g. token, SMS texting, etc.).

- Click **Sign On**.

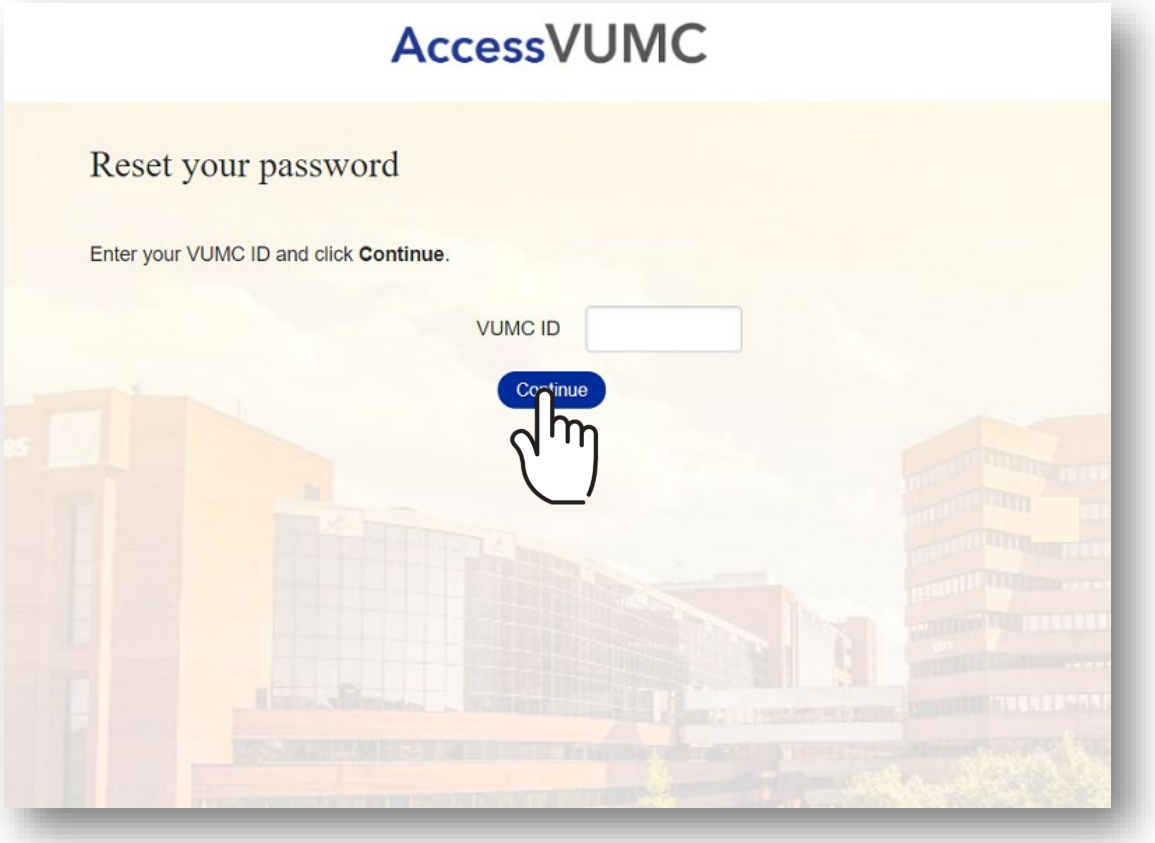
MFA Sign on for SMS Text users



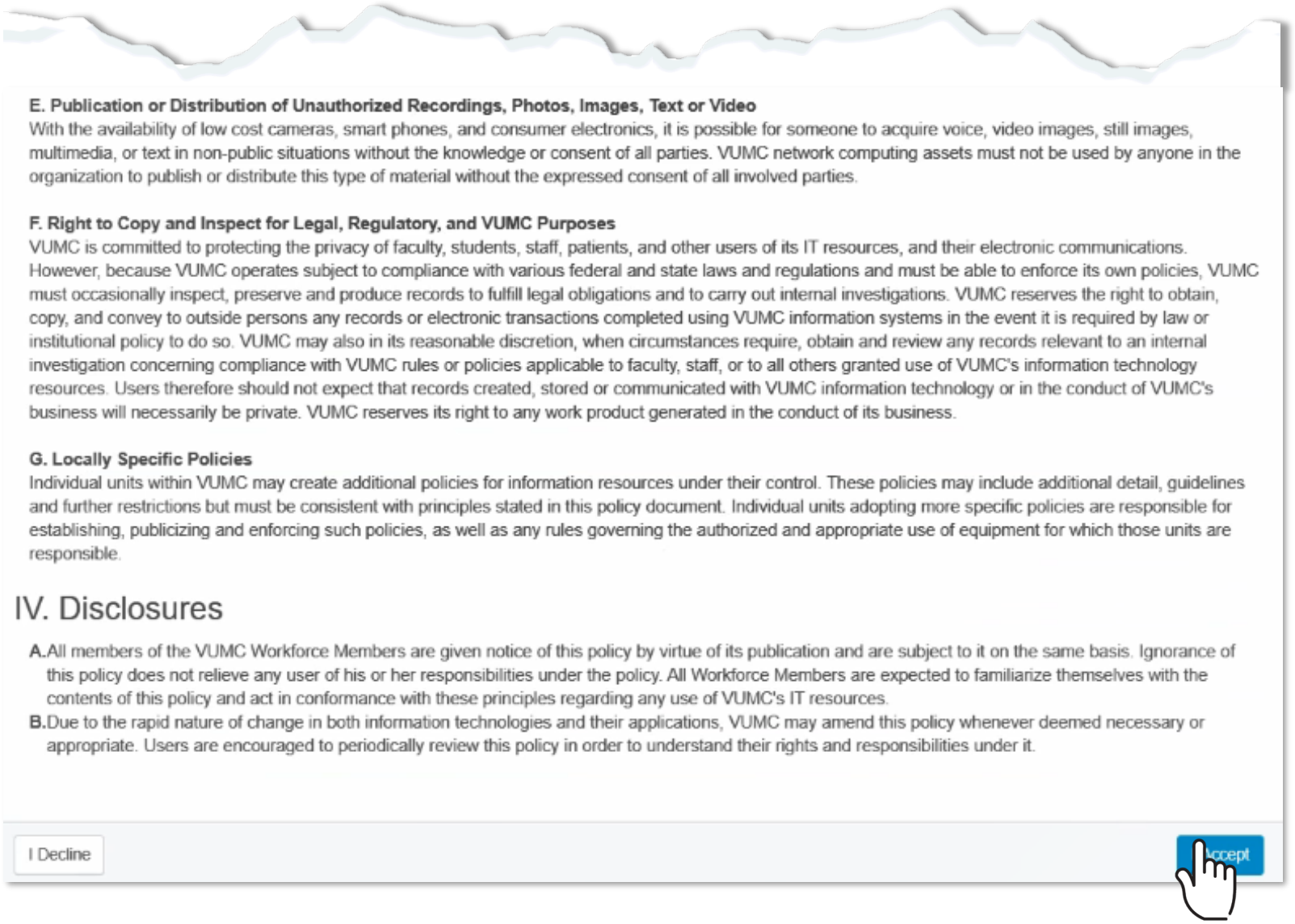
MFA Sign on for Token users



- Verify your identity by entering your VUMC ID.
- Click **Continue**.



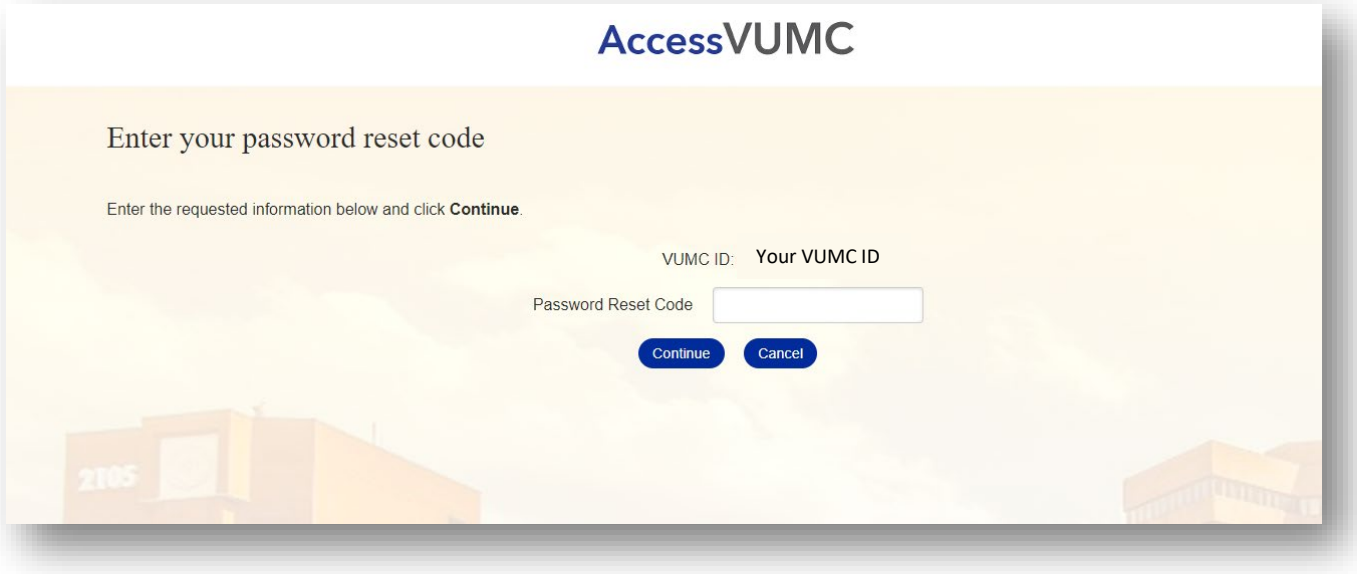
Click **Accept** once you have read the VUMC Acceptable Use Policy regarding your computer privileges and responsibilities.



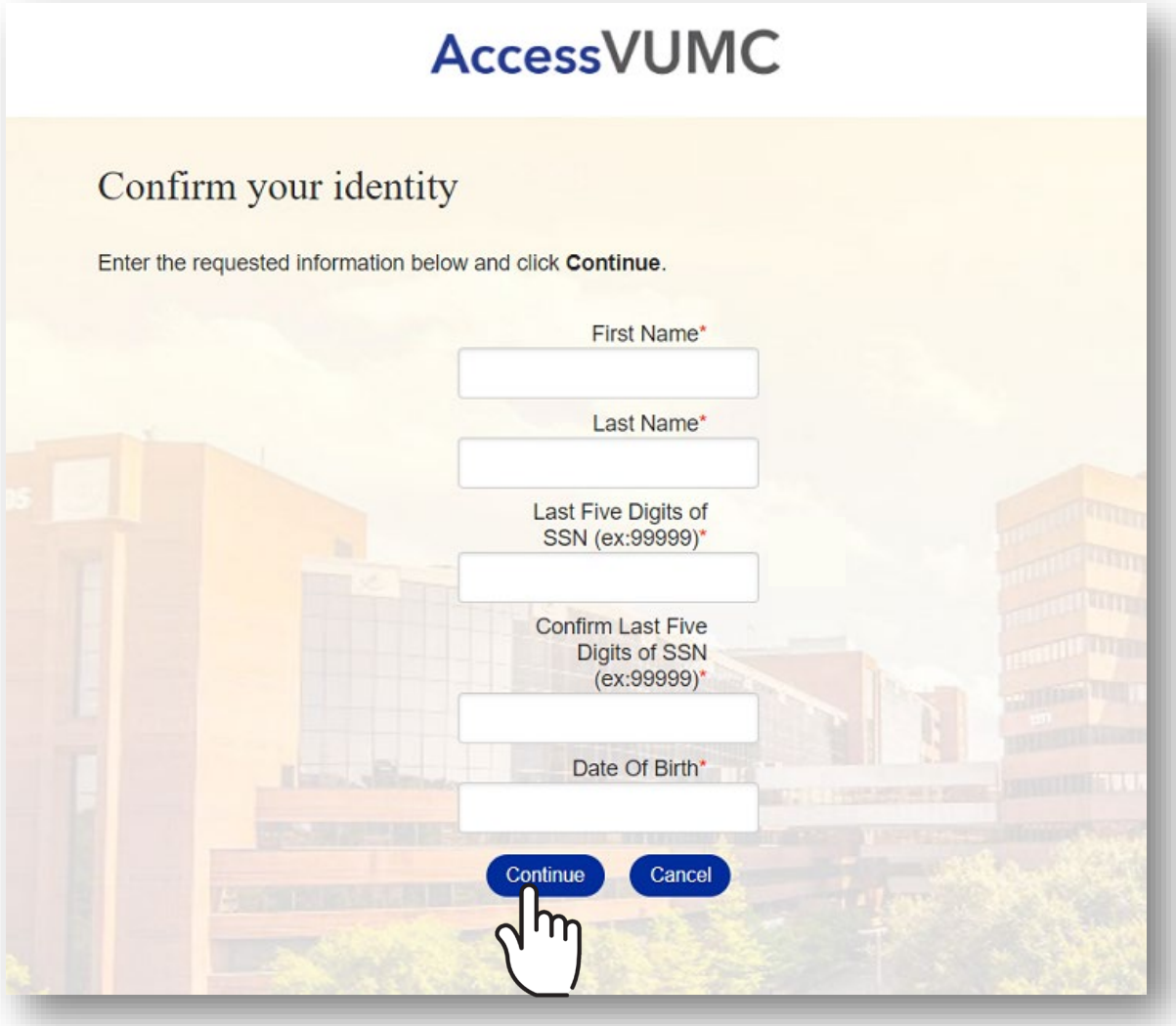
Reset a Password

For ACTIVE VUMC ID HOLDERS enrolled in Multi-Factor Authentication

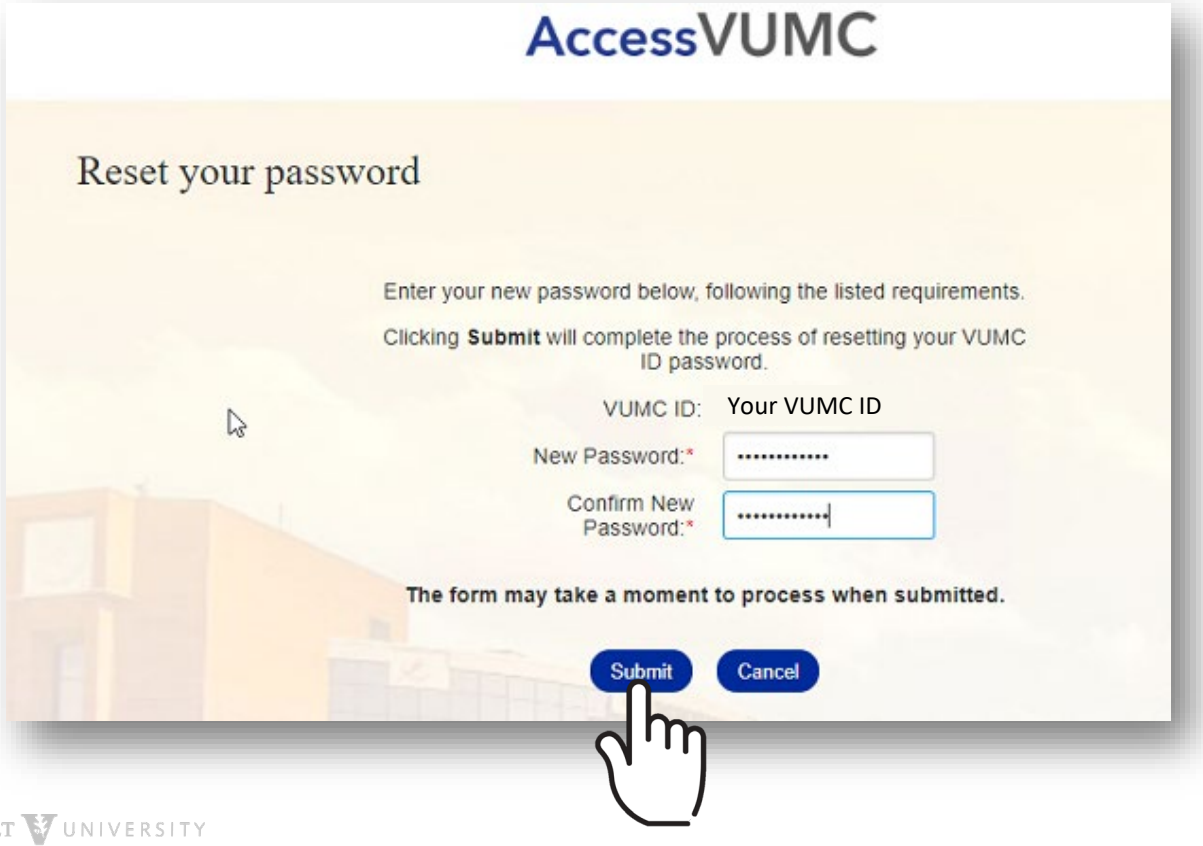
- If you receive the screen below, then you have not yet entered your Personal Identifiable Information (PII).
- Your PII is required to reset your password.
- Call the VUMC IT/NTT Help Desk at 615-343-HELP/3-4357 to get a one-time passcode.
- Use your one-time passcode to sign on at any time, follow the same steps, and, once you arrive at this screen, enter the code and click **Continue**.
- You can then follow the remaining instructions to reset your password.



- Confirm your identity by entering your personal identifiable information (PII).
- Click **Continue**.



- Enter your new password and confirm.
- Click **Submit**.



Keep these 3 password basics in mind when you create your VUMC Account password.

1. You cannot reuse your last 10 passwords
2. Passwords MUST CONTAIN:
   - At most 16 characters
   - At least 1 lowercase letter
   - At least 8 characters
   - At least 3 character types
   - At least 1 number
   - At least 1 uppercase letter
3. Passwords CANNOT CONTAIN your:
   - Email address
   - Account last name
   - Display name
   - Account names in reverse

- You will receive a confirmation screen that your password was successfully re-authenticated.
- You will also receive an email that your password was changed.
- Click **Finish**.

Reset a Password

For VUMC EMPLOYEES or VUMC ID HOLDERS NOT ENROLLED in Multi-Factor Authentication

AccessVUMC Identity Management

Return to “Reset Password” Menu

Reset a Password

For VUMC EMPLOYEES and ACTIVE VUMC ID HOLDERS
NOT ENROLLED in Multi-Factor Authentication

If you are a VUMC employee or active VUMC ID holder and are **NOT** enrolled in Multi-Factor Authentication, contact the VUMC IT/NTT Help Desk at 615-343-HELP/3-4357 to start the Password Reset (reauthentication) Process.

You will receive a temporary password that will be valid for three days.

Use the temporary password to login to MyMFA and enroll in Multi-Factor Authentication. Enroll in MFA.

After enrolling in MFA, follow the steps from slide #8 and go through regular change password process. Go to Slide #8.