SMALL BUSINESS/SMALL DIVERSE BUSINESS APPLICATION INSTRUCTIONS
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Requirements</td>
<td>4</td>
</tr>
<tr>
<td>Quick Access Instructions</td>
<td>5</td>
</tr>
<tr>
<td>Small Business</td>
<td>5</td>
</tr>
<tr>
<td>Small Diverse Business</td>
<td>5</td>
</tr>
<tr>
<td>Instructions</td>
<td>6</td>
</tr>
<tr>
<td>Small Diverse Business Verification</td>
<td>17</td>
</tr>
<tr>
<td>Troubleshooting Tips</td>
<td>20</td>
</tr>
<tr>
<td>Compatibility Mode</td>
<td>21</td>
</tr>
<tr>
<td>Additional Settings for IE 11.0</td>
<td>23</td>
</tr>
<tr>
<td>Viewing Secure and Nonsecure Content</td>
<td>28</td>
</tr>
<tr>
<td>Windows 10 with Microsoft Edge</td>
<td>29</td>
</tr>
<tr>
<td>Other Browsers, Operating Systems, and Technology</td>
<td>30</td>
</tr>
<tr>
<td>Firefox – PC and Macintosh</td>
<td>30</td>
</tr>
<tr>
<td>Google Chrome – PC &amp; Macintosh</td>
<td>31</td>
</tr>
<tr>
<td>Safari - Macintosh</td>
<td>33</td>
</tr>
</tbody>
</table>

_Bureau of Diversity, Inclusion & Small Business Opportunities_  
North Office Building  
401 North Street, Room 611  
Harrisburg, PA 17120-0500  
717.783.3119 (O) | 717.787.7052 (F)  
gs-bdisbo@pa.gov
Quick Contact List:

Login Problems: Select “Forgot Your Password?” or “Forgot Your UserID?” on the Log On page, or contact the Supplier Service Center at ra-pscsrmportal@pa.gov (preferred) or (877) 435-7363, option 1, or visit the PA Supplier Portal Administrator Support page for additional troubleshooting tips and how-to guides.

Enterprise Applications (Blank page after following Troubleshooting Tips): Visit http://www.budget.pa.gov/Services/ForVendors/Pages/PASP-Admin-Support.aspx > “Troubleshoot for a Blank or White Screen” or contact the Supplier Service Center at ra-pscsrmportal@pa.gov (preferred) or 877.435.7363, Option 1.

Upload Issues: Bureau of Diversity, Inclusion & Small Business Opportunities, 717.783.3119, RA-SmallBusiness@pa.gov.

Online Application Questions (Steps 1 – 7 of online application): Bureau of Diversity, Inclusion & Small Business Opportunities (BDISBO), 717.783.3119, RA-SmallBusiness@pa.gov or GS-BDISBO@pa.gov.
## SYSTEM REQUIREMENTS

<table>
<thead>
<tr>
<th>Certified Browsers</th>
<th>Internet Explorer 8.0, 9.0, 10.0, 11.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Operating Systems</td>
<td>Microsoft Windows 7.0, 8.0, 8.1</td>
</tr>
<tr>
<td>(See important notice regarding Windows 10 below)</td>
<td></td>
</tr>
<tr>
<td>Technology</td>
<td>PCs</td>
</tr>
<tr>
<td>Other Browsers, Operating Systems &amp; Technology</td>
<td>Full functionality not assured</td>
</tr>
</tbody>
</table>

NOTE: The PA Supplier Portal may work with other Browsers, Operating Systems, and Technology. See the Other Browsers, Operating Systems, and Technology in the Troubleshooting Tips section of this guide.

### IMPORTANT NOTICE: Windows 10 Known Compatibility Issues

In August 2015, Microsoft released its Windows 10 operating system along with a new Internet browser called Edge. This operating system and web browser have been integrated in many commonwealth business partner IT environments. However, several compatibility issues are known to remain. Follow the troubleshooting instructions on page 30 of this guide if using the Edge browser in Windows 10.
QUICK ACCESS INSTRUCTIONS

Visit the PA Supplier Portal Administrator Support page for additional troubleshooting tips and how-to guides such as Confirming Website and Browser Compatibility, Troubleshooting for a Blank or White Screen, Resetting a Password, Creating Additional Users, Editing or Updating the Company Name on the Vendor Registration, Changing Administrative User Information, Editing or Changing Other (Non-Administrative) Users’ Information, Changing the Tax Identification Number, Changing the Administrative User Email Address on the Vendor Registration When Unable to Reset the Password, and more.

SMALL BUSINESS

1. Go to the PA Supplier Portal at www.pasupplierportal.state.pa.us.
2. Click the Log on button in the upper right and login. TIP: If you do not know your password or User ID, select “Forgot Your Password?” or “Forgot Your UserID?” on the Log On page, or contact the Supplier Service Center at ra-pcsrmportal@pa.gov (preferred) or (877) 435-7363, option 1.
3. Click “Bidder” → “Enterprise Applications” → “Small & Small Diverse Business Program Application”.
4. Scroll to the bottom of the page, check the box, and click “Continue to Self-Certification” or “Continue to Recertification”.
5. Click through any pop-up boxes to enter the application.

SMALL DIVERSE BUSINESS

1. Follow the Small Business instructions above to access the Small Business Application.
2. If you’ve just submitted a new small business certification or a recertification: Scroll down to the bottom of the Congratulations page and click Yes at “Do you also wish to verify as a Small Diverse Business?” TIP: If this page does not appear, follow the instruction on the next line.

OR

Click the Step 5 tab, and click on the “Verify as an SDB” button at the bottom of the page.
3. Upload your third-party proof of certification in Step 6, click “Save”, and then click “Save and Continue”. Repeat for all third-party certifications if you are submitting more than one. TIP: The UCP, SBA 8(a), and VetBiz verifications have two or three fields for the upload of documentation. All fields must be completed for these verifications before saving.

As a reminder, BDISBO no longer directly certifies Minority, Woman, Veteran, Service Disabled Veteran, LGBT, or Disability-owned businesses. You must have a current certification from one of seven approved third-party organizations. Find the list at www.dgs.pa.gov → BUSINESSES → SMALL DIVERSE BUSINESS PROGRAM → SMALL DIVERSE BUSINESS VERIFICATION. If you are renewing your Small Diverse Business verification and you have submitted an application to a new third-party certifier or recertification application to your current third-party certifier but it is still in process, you may complete the AFFIDAVIT TO REQUEST EXTENSION FOR SMALL DIVERSE BUSINESS DESIGNATION to submit in place of the certification while it is still in process. It will act as a placeholder until the application is approved and you can forward the proof of third party certification. Contact BDISBO at GS-SmallBusiness@pa.gov or 717.783.3119 for a copy of the affidavit.
1. Enter www.pasupplierportal.state.pa.us in address bar at top of screen.
2. You should now be on the PA Supplier Portal. Click on the Log on button at the top right.
3. Login with your User Name and Password. Select “Forgot Your Password?” or “Forgot Your UserID?” on the Log On page, or contact the Supplier Service Center at ra-pscsrmportal@pa.gov (preferred) or (877) 435-7363, option 1, or visit the PA Supplier Portal Administrator Support page for additional troubleshooting tips and how-to guides.
4. Once logged in, select the **Bidder** tab.
5. Click on “Enterprise Applications”. See the next page if a security warning appears.

If this page is blank after selecting Enterprise Applications, logout and log back into the application, click on Vendor Administrator tab (to the left of the Bidder tab) → Bidder tab → Enterprise Applications → Small & Small Diverse Business Program Application.

OTHER POSSIBLE ISSUES

- You have not given permission to view all content.
- You are not using Internet Explorer (IE) 8.0, 9.0, 10.0, or 11.0.
- You are using IE 11.0 but running it in Compatibility Mode hasn’t resolved the problem.
- You are running Windows 10 (run Windows 7).
- You are using a Mac system.

See the Troubleshooting Tips at the end of this guide. For additional tips, visit the PA Supplier Portal Administrator Support page.

CONTACT THE SUPPLIER SERVICE CENTER AT RA-PSCSRMPORTAL@pa.gov (PREFERRED) OR 877-435-7363, OPTION 1 IF YOU CONTINUE EXPERIENCING ISSUES AFTER FOLLOWING THE TROUBLESHOOTING TIPS.
6. If a security box pops up, hit “Yes” if it looks like this . . .

![Security Information]

... or “No” if it looks like this.

![Security Warning]

Or click the “Show all content” button if this appears at the bottom of the window. NOTE: Click “Show all content” may route you back to the Welcome Vendor Administrator page. Click Bidder > Enterprise Applications again if this happens.

![Only secure content is displayed.]

If the security warning does not appear, continue to the next step. It may appear later in the process. If it does, follow the directions above. The goal is to be able to view all information, secure and nonsecure. For additional pointers, please see the Troubleshooting Tips for Viewing Secure and Nonsecure Content at the end of this guide.
7. Click on Small & Small Diverse Business Program Application.
8. You have reached the application welcome screen. Scroll down to the bottom of the page, check the box.

---

**Welcome XYZ ENTERPRISES**

**Eligibility Requirements**

Businesses interested in participating in the Small and Small Diverse Business Programs must first become certified as a Small Business. To self-certify, a business must meet each of the following requirements:

- The business must be a for-profit, United States business.
- The business must be independently owned.
- The business may not be dominant in its field of operation.
- The business may not be a subsidiary of another business.
- The business may not employ more than 100 full-time equivalent employees.
- The business, by type, may not exceed the following three-year average gross sales:

---

- A determination by the procuring agency that a bidder is not responsible as found in Management Directive 215.9, Commonwealth Contractor Responsibility Program.
- A determination by the procuring agency to terminate any contract entered into with the agency; and/or
- Criminal prosecution and/or any other legal actions permitted by law.

**By checking this box, I certify that I have read the Program Overview and Eligibility Requirements, and I fully understand the potential consequences of providing false information as a part of this self-certification process.**

[Continue to Self-Certification] [No Thanks] Note: Clicking No Thanks will redirect you back to the DGS website.
9. Click the **Continue to Self-Certification** button in the Confirmation box.
10. Once in the application, you can navigate to a given Step by clicking the appropriate tab at the top of the application. If you have not yet started the application, you will begin in Step 1. If you have already submitted the application, Steps 1 and 4 will be locked. You must contact the Bureau of Diversity, Inclusion & Small Business Opportunities at RA-smallbusiness@pa.gov to request that they be unlocked for editing.

NOTE: Every step must be completed to self-certify or recertify. Click Save and Continue at the bottom of each page to continue from step to step upon initial certification and recertification to ensure no required data is missing. Your company’s certification will not be approved or appear in the online directory until all required data has been entered and saved.

Do not use your browser’s back button. Simply click the appropriate Step button from the black bar above.
11. Review and submit the application in Step 5 by checking the boxes at the bottom of the page, entering a Signature and Title, and clicking “I Acknowledge and Electronically sign.”
This step is required only for those companies wishing to verify as a Minority, Woman, Veteran, Service-Disabled Veteran, LGBT, and/or Disability-Owned Business Enterprise through the Small Diverse Business (SDB) program. Those self-certifying as Small Business only may stop here.

NOTE: You must have proof of a current certification from an approved third-party certifier available for upload to complete the following steps. Go to [www.dgs.pa.gov → BUSINESSES → SMALL DIVERSE BUSINESS PROGRAM](http://www.dgs.pa.gov) for a current list of approved certifiers.

1a. The Small Diverse Business verification application is accessible through the Small Business Self-Certification application. If you have just submitted your small business self-certification, click [Continue to SDB Verification](#) at the bottom of the Congratulations page.
1b. If you submitted your small business self-certification at an earlier time or the Congratulations page does not appear, click the Step 5 tab and then the **Verify as an SDB** button which will appear at the bottom of the page. NOTE: This button will not appear until the small business self-certification or recertification has been completed and submitted.

Do not use your browser’s back button. Simply click the appropriate Step button from the black bar above.

Verification of Small Diverse Business Status

Step 6
Please select the third-party certification(s) for which your business is seeking verification. Multiple third-party certifications may be selected; however, the supporting documentation listed will be required for each third-party certification for which your business seeks verification. Expired certifications from any entity will not be accepted.

- Uniform/Unified Certification Program (UCP): (Click to show details...)

- National Minority Supplier Development Council (NMSDC): (Click to show details...)
TROUBLESHOOTING TIPS

COMPATIBILITY MODE

ADDITIONAL SETTINGS FOR IE 11.0

VIEWING SECURE AND NONSECURE CONTENT

OTHER BROWSERS, OPERATING SYSTEMS, AND TECHNOLOGY
To determine what version of Internet Explorer you are using, click **Help → About Internet Explorer**.

OR

Click the **About Internet Explorer** button.
INTERNET EXPLORER

The PA Supplier Portal is compatible with the Internet Explorer (IE) browser versions 8.0, 9.0, 10.0, and 11.0. If you are running IE 10.0 or 11.0, you may need to run it in Compatibility Mode:

Click this button ( ) if it appears in the Address Bar.

OR

1. Open Internet Explorer.
2. Press the Alt key to display the Menu bar (or right–click the Address bar and then select Menu bar).
3. Click Tools → Compatibility View settings (ALT + T + B).

OR

1. Press the Alt key to display the Menu bar (or right–click the Address bar and then select Menu bar).
2. Click Tools (alternatively you can just press the F12 key on your keyboard)
3. Click Browser Mode and then click on the Internet Explorer version you want to simulate.

OR (Internet Explorer 11)

1. Tap or click the Tools button → Compatibility View settings.
2. Under Add this website, enter the URL of the site you want to add to the list, and then tap or click Add.

PLEASE USE A COMPATIBLE BROWSER, (IE 8.0, 9.0, 10.0, OR 11.0) FOR COMPATIBILITY.
If you continue experiencing issues while using IE 11.0, try the following Internet options settings.

1. Tap or click the **Tools** button, and then tap or click **Internet options**.
SECURITY TAB – INTERNET

Select a zone to view or change security settings.

- Internet
  - This zone is for Internet websites, except those listed in trusted and restricted zones.
  - Security level for this zone: Custom
    - Custom settings.
    - To change the settings, click Custom level.
    - To use the recommended settings, click Default level.
- Local intranet
  - Trusted sites
  - Restricted sites

- Sites
- Reset all zones to default level

SECURITY TAB – LOCAL INTRANET

Select a zone to view or change security settings.

- Internet
  - Trusted sites
  - Restricted sites

- Local intranet
  - This zone is for all websites that are found on your intranet.

- Security level for this zone: Medium-low
  - Appropriate for websites on your local network (intranet)
  - Most content will be run without prompting you
  - Unsigned ActiveX controls will not be downloaded
  - Same as Medium level without prompts

- Enable Protected Mode (requires restarting Internet Explorer)
- Custom level...
- Default level
- Reset all zones to default level
SECURITY TAB – TRUSTED SITES

Select a zone to view or change security settings.

Internet Local intranet Trusted sites Restricted sites

Trusted sites
This zone contains websites that you trust not to damage your computer or your files.

Security level for this zone
Allowed levels for this zone: All

Medium
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

[ ] Enable Protected Mode (requires restarting Internet Explorer)

TRUSTED SITES AFTER SELECTING “SITES”

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Websites:
https://www.google.com

[ ] Require server verification (https:) for all sites in this zone

Close
## Advanced Settings

- **Accelerated graphics**
  - Use software rendering instead of GPU rendering

- **Accessibility**
  - Always expand ALT text for images
  - Enable Caret Browsing for new windows and tabs
  - Move system caret with focus/selection changes
  - Play system sounds
  - Reset text size to medium for new windows and tabs
  - Reset zoom level for new windows and tabs

- **Browsing**
  - Always record developer console messages
  - Close unused folders in History and Favorites
  - Disable script debugging (Internet Explorer)
  - Display a notification about every script error
  - Enable automatic crash recovery
  - Enable flip ahead with page prediction
  - Enable FTP folder view (outside of Internet Explorer)
  - Enable Suggested Sites
  - Enable third-party browser extensions
  - Enable visual styles on buttons and controls in webpages
  - Go to an intranet site for a single word entry in the Address bar
  - Load sites and content in the background to optimize performance
  - Notify when downloads complete
  - Show friendly HTTP error messages
  - Tell me if Internet Explorer is not the default web browser

- **Underline links**
  - Always
  - Hover
  - Never

- **Use inline AutoComplete in File Explorer and Run Dialog**
  - Use inline AutoComplete in the Internet Explorer Address
  - Use most recent order when switching tabs with Ctrl+Tab
  - Use Passive FTP (for firewall and DSL modem compatibility)
  - Use smooth scrolling

- **HTTP settings**
  - Use HTTP 1.1
  - Use HTTP 1.1 through proxy connections
  - Use SPDY/3

## Advanced Settings Continued

### International
- Always show encoded addresses
- Send IDN server names for Intranet URLs
- Send IDN server names for non-Intranet URLs
- Send URL path as UTF-8
- Send UTF-8 query strings for Intranet URLs
- Send UTF-8 query strings for non-Intranet URLs
- Show Notification bar for encoded addresses

### Multimedia
- Enable alternative codecs in HTML5 media elements
- Enable automatic image resizing
- Play animations in webpages
- Play sounds in webpages
- Show media download placeholders
- Show pictures

### Security
- Allow active content from CDs to run on My Computer
- Allow active content to run in files on My Computer
- Allow software to run or install even if the signature is invalid
- Block unsecured images with other mixed content
- Check for publisher's certificate revocation
- Check for server certificate revocation
- Check for signatures on downloaded programs
- Do not save encrypted pages to disk
- Empty Temporary Internet Files folder when browser is closed
- Enable 64-bit processes for Enhanced Protected Mode
- Enable DOM Storage
- Enable Enhanced Protected Mode
- Enable Integrated Windows Authentication
- Enable native XMLHttpRequest support
- Enable SmartScreen Filter
- Enable Strict P3P Validation
- Send Do Not Track requests to sites you visit in Internet Explorer
  - Use SSL 2.0
  - Use SSL 3.0
  - Use TLS 1.0
  - Use TLS 1.1
  - Use TLS 1.2
  - Warn about certificate address mismatch
  - Warn if changing between secure and not secure mode
  - Warn if POST submittal is redirected to a zone that does not require authentication
2. The following Security warning message appears at the bottom of the screen when returning to Enterprise Applications. Select Show all content.

![Security Warning Message](image)

3. You will be returned back to the welcome vendor administrator page. Hit the Bidder Tab > Enterprise Applications > Small & Small Diverse Business Program Application.

![Vendor Administrator Page](image)
VIEWING SECURE AND NONSECURE CONTENT

When viewing a website in Internet Explorer 9 or later, you receive a message that reads "Only secure content is displayed."

This message is telling you that there may be both secure and non-secure content on the page. Secure and non-secure content, or mixed content, means that a webpage is trying to display elements using both secure (HTTPS/SSL) and non-secure (HTTP) web server connections. This often happens with online stores or financial sites that display images, banners, or scripts that are coming from a server that is not secured. The risk of displaying mixed content is that a non-secure webpage or script might be able to access information from the secure content.

INTERNET EXPLORER BLOCKS NON-SECURE CONTENT BY DEFAULT and is set to prompt you when this is happening.

WINDOWS 7, WINDOWS VISTA, AND WINDOWS XP

To Disable/Enable/Prompt the “Only secure content is displayed” message:

1. Start Internet Explorer.
2. On the Tools menu, click Internet Options.
3. Click the Security tab, and then click Internet and then Custom Level.
4. In the Settings box, scroll down to the Miscellaneous section, and under Display mixed content choose from the following options:
   - Disable, will not display non-secure items.*
   - Enable, will always display non-secure items without asking
   - Prompt, will prompt you when a webpage is using non-secure content

WINDOWS 8

To Disable/Enable/Prompt the “Only secure content is displayed” message:

1. From the start screen, type Internet Options.
2. Tap or click the Settings option below the Search box, and then tap or click Internet Options.
3. Tap or click the Security tab, and then tap or click Custom Level.
4. In the Settings box, scroll down to the Miscellaneous section, and under Display mixed content choose from the following options:
   - Disable, will not display non-secure items.*
   - Enable, will always display non-secure items without asking
   - Prompt, will prompt you when a webpage is using non-secure content

*If Display mixed content is set to Disable, select Enable or Prompt. If it is set to Prompt and all contact is still not displayed, set to Enable.

Internet Explorer blocks non-secure content to keep your information safe and is set to Prompt by default. When this setting is set to Enable, Internet Explorer does not prompt you with the "Only secure content is displayed" message even if the webpage is using non-secure elements.

NOTE: If you are still logged into the PA Supplier Portal when resetting the Display mixed content setting, please log out and log back in to be able to view content based on the new setting.
1. Tap the three-dot menu button on the top right on any page that you want to open in Internet Explorer.
2. Select "Open with Internet Explorer"
OTHER BROWSERS, OPERATING SYSTEMS, AND TECHNOLOGY

Full functionality with the PA Supplier Portal is guaranteed only when certain system requirements have been met. However, in some situations, the following tips may allow the PA Supplier Portal to function on other browsers, operating systems, and technology.

Firefox – PC and Macintosh

Mixed Content

HTTP is a system for transmitting information from a web server to your browser. HTTP is not secure. When you visit a page fully transmitted over HTTPS, you'll see a green padlock icon in the address bar. This means that your connection is authenticated, encrypted, and safeguarded. However, if the HTTPS page you visit includes HTTP content, the HTTP portion can be read or modified by attackers, even though the main page is served over HTTPS. When an HTTPS page has HTTP content, we call that content “mixed”. The page you are visiting is only partially encrypted and even though it appears to be secure, it isn't.

Firefox blocks mixed content by default. It does not provide a message to the users, so they may not know that the content is being blocked by the browser. In addition, the block appears at the page level, so you may need to unblock pages more than once while working on different content pages.

To tell if a page has mixed content, look for an icon to the left in the address bar:

- You are on a fully secure page. To see if Firefox has blocked parts of the page that are not secure, click the green lock icon.
- Firefox is not blocking insecure elements. Unless you’ve unblocked mixed content, you shouldn’t see this icon.
- Firefox is not blocking insecure passive content.

Unblocking insecure elements is not recommended, but can be done if necessary:

1. Click the lock icon in the address bar (check for an exclamation point if the lock icon does not appear).

2. Click the arrow on the Control Center:
3. Click **Disable protection for now.**

4. To enable protection, follow the preceding steps and click **Enable protection.**

---

**Blank Screens**

A blank screen is the result of a security feature in Google Chrome called Mixed Content Blocking. This feature blocks non-https content from displaying in an https page by default unless specifically allowed during each page visit.

Chrome version 21 or later blocks mixed content by default. It does not provide a message to the users, so they may not know that the content is being blocked by the browser. The block appears at the page level, so you may need to unblock pages more than once while working on different content pages.

To allow all content to display in Google Chrome:

1. Check the upper right corner of your screen for the Shield icon. This icon indicates that Google Chrome has blocked the page from displaying.

OR
2. Click on the Shield icon and a box will pop-up asking if you want to “Load unsafe script”. Click the “Load unsafe script” or “Load anyway” text to allow the page to display.

3. Google Chrome will refresh your screen; you will need to navigate back to “Bidder” → “Enterprise Applications” → “Small & Small Diverse Business Program Application”.
4. Now when you click the link, the page should display. The address bar in your browser will display the https URL in red with a line through it to denote that mixed content is being displayed in Google Chrome.

5. Note: Due to the security in Google Chrome, you will have to follow this process every time you encounter the blank screen and see the Shield icon in the upper right corner of your screen.

To set your Chrome browser to always allow mixed content (Note: If using this option, Chrome will no longer check for unsecured content for any website or webpage.)

1. In an open Chrome browser, press Ctrl + Shift + Q on your keyboard to force close Chrome. Chrome must be fully closed before the next steps.
2. Right-click the Google Chrome desktop icon (or Start Menu link).
4. At the end of the existing information in the Target field, add: " --allow-running-insecure-content" (There is a space before the first dash.)
5. Click OK.
6. Open Chrome and try to launch the content that was blocked earlier.

NOTE: These instructions may not work for Google Chrome versions 34 and 35. To update to the most current version of Google Chrome, open Chrome, click the three vertical dots in the upper right corner, and click Update Google Chrome (if you don’t see this button, you’re on the latest version). Click Relaunch once complete.
The PA Supplier Portal is not compatible with Mac systems; however, users have had success accessing the Supplier Portal following the instructions below.

1. Open Safari > Preferences from the menu bar.
2. Click on the Advanced tab.
3. At the bottom, check the “Show Develop menu in menu bar” box.
4. Quit and relaunch Safari.
5. From the top menu bar, go to Develop > User Agent and select “Google Chrome – Windows”.
6. Log into the PA Supplier Portal.
7. From the top menu bar, go to Develop > Show Error Console.

8. In the Error Console, click the link http://www.dgs.internet.state.pa.us/ITQ_Vendor/Welcome.aspx to display insecure data content.