

Office of Security Administration

The Office of Security Administration partners with staff across the Division of Finance and Administration to develop and support processes that strengthen internal controls, ensure compliance, promote best practices in higher education, and enhance overall efficiency and effectiveness. To contact the Office of Operational Excellence, send an email to cpi-security@astate.edu.

- [Pre-Security Requirements](#)
- [Security](#)
- [VPAT-Technology Accessibility](#)
- [Tips and Troubleshooting](#)
- [Training Guides & Information](#)

Pre-Security Requirements

All employees are required to complete the following courses in the [Employee Learn Center](#) module within their first 30 days of employment.

- Child Maltreatment
- Title IX (Sexual Discrimination)
- Privacy and Security
- FERPA

Once the required training module has been completed, the appropriate security request form may be submitted.

Security

[Banner Access Security Form](#) Utilized for finance initiator/approvers, supervisors and leave/time approvers and their proxies, travel and expense, and student accounts receivable access. Please contact cpi-security@astate.edu for further assistance with Finance and Travel security.

Banner Student Security – Maintained by the Registrar’s Office for Banner Student module access. FERPA training is required for employees who request access to student information. Please contact registrar@astate.edu for further assistance with Banner Student security.

[Non-Employee Sponsored Account](#)– Submitted by an Employee who is sponsoring a non-employee/privatized employee for an A-State account and/or system access. Any individual who is not paid by the University and needs access must be set up through this process.

VPAT-Technology Accessibility

When purchasing web or other IT products, departments must ensure that they are accessible to everyone, including users with disabilities.

The State of Arkansas is required to comply with the provisions of Arkansas Code Annotated §25-26-201 et seq., as amended by [Act 308 of 2013](#) and the Government-wide [Section 508](#) Accessibility Program prior to procuring a technology product or when soliciting the development of such a product. Arkansas Code §25-26-201 expresses the policy of the State to provide individuals who are blind or visually impaired with access to information technology purchased in whole or in part with state funds.

Departments are responsible for obtaining a Voluntary Product Accessibility Template (VPAT®) from the vendor and submitting the required documentation for review prior to the procurement of such technology.

VPAT Review Process

VPAT® (Voluntary Product Accessibility Template) is a template used to document a product's conformance with accessibility standards and guidelines.

- **For web-based products**, the accepted VPAT® is the current [WCAG Edition](#) made available from the [Information Technology Industry Council](#)
- **For other products**, the accepted VPAT® is the current [Revised Section 508 Edition](#) available from the [Information Technology Industry Council](#)

When requesting a quote for a technology purchase please ask the vendor if they have a VPAT® or if they are willing to complete one. If they cannot, the process can continue, but it is recommended that an alternative vendor and/or product be sought. You can also try doing a web search for the terms "508" or "VPAT" along with the product and/or vendor name as many manufacturers publish these documents to their websites.

First, review the VPAT® and if "Partially Supports" or "Does Not Support" appears in the column then the product is not fully accessible. Ask the vendor for a remediation road map if this is the case.

Second, a basic accessibility evaluation consists of testing out usage of the product with keyboard-only navigation and compatibility with screen reading software. Tools to complete this can be found in #3.

One of the following checklists can be completed, with optimum effort, to aid in the overall VPAT® evaluation:

- [Software Accessibility Checklist](#)
- [Web Accessibility Checklist](#)

For assistance in completing these checklists, please contact Marcus Carlton at **972-2011** or vp@astate.edu.

In order for our office to evaluate, we must have a demo or trial version of the product. Simply provide a link and/or provide any login credentials for the demo and send to vp@astate.edu.

The following resources can be used to assist in completion of VPAT® testing:

Screen Readers

- Desktop Software, Web Sites, or Web Services: [JAWS](#), [NVDA](#), [Apple Voiceover](#)
- Mobile software: [Android Accessibility](#) for Android or [Voiceover](#) for iOS are default programs

Keyboard

- [Windows](#) shortcuts
- [Mac](#) shortcuts

Magnifiers

- [Windows](#) magnifiers
- [Mac](#) zoom

Site Scans

- Use [WAVE \(Web Accessibility Evaluation Tool\)](#) to scan web sites for accessibility flaws

Testing Tools for Web

- ANDI (Accessible Name & Description Inspector)
 - free open-source bookmarklet, which means that the tool does not require installation as a plugin and can be added to multiple browsers as a bookmark. [Install ANDI](#)
- Color Contrast Analyzer (CCA)
 - free open-source tool that displays the contrast ratio for two selected colors. CCA is used to inspect color contrast when contrast cannot be programmatically identified by ANDI.
 - [CCA 2.5 for Windows](#)

- [CCA 2.4 for macOS](#)

The [Technology Accessibility Overview Form](#) should be completed for every VPAT® evaluation request. The form asks details such as requestor information, technology details, and contains the approval signature. It is used to provide details that may aid in the overall evaluation. Once completed, a copy of the form will be automatically sent to our office.

Submit all VPATs and other documents, as well as the information to download or log into a demo to vpap@astate.edu or hand deliver the documents to the Administration Building - Office of Finance, Attention: George Hannah or Marcus Carlton.

Once the product has been approved for accessibility and other criteria met, the department may submit a Banner requisition to Procurement Services.

- Once the product has been approved for accessibility and other criteria met, the department may submit a Banner requisition to Procurement Services.
- **All technology purchases must have an [ASU ITS Security Questionnaire](#) completed by the vendor or on file before the purchase can be made. Contact the [Information Technology Security](#) team for questions and to submit.**
- **For all types of technology, Pcard usage must be approved by Procurement Services before the purchase can be made.**
-

Tips and Troubleshooting

BROWSER

For each browser(s) used, follow the steps below to resolve common issues. It is recommended that the computer be restarted following any changes.

[SETTING THE BROWSER TO CLEAR CACHE WHEN CLOSING](#)

Chrome:

1. Open the Chrome browser.
2. Open the Chrome Toolbar (3 lines to the right of the URL window) and then select **Settings**.
3. Select **Show advanced settings....**
4. Click the **Content Settings button** located under the Privacy section.
5. Under the first section labeled Cookies, select **Keep local data only until you quit your browser**.
6. Click **Done**.

Firefox:

1. At the top of the Firefox window, click the Firefox button and then select **Options**.
2. Select the Privacy panel.
3. In the *History* section, set **Firefox will:** to **Use custom settings for history**.
4. Select the checkbox for **Clear history when Firefox closes**.
5. Click the **Settings...** button. The Settings for Clearing History window will open.
6. In the Settings for Clearing History window, click the checkmark box next to **Cache**.
7. Click **OK**.

Internet Explorer:

1. Open the IE browser.
2. Click **Tools > Internet Options > Advanced** tab.
3. Scroll down to the Security section and then check the box: **Empty Temporary Internet Files folder when browser is closed**.
4. Click **OK**.

[ALLOWING POP-UPS IN BROWSERS](#)

Chrome:

1. To the far right of the address bar click the ellipsis.
2. At the bottom of the **Settings** page click **Advanced**.
3. Under the Privacy and Security section click **Content Settings > Pop-ups and redirects**.
4. Enable or disable the slider to block or allow all pop-ups. Additionally specific sites can be blocked or allowed.

Firefox:

1. To the far right of the address bar click the Open Menu icon.
2. Click **Options**.
3. Click **Privacy and Security** from the menu and under Permissions, either check or uncheck the box labeled "Block pop-up windows."

Safari:

1. Click **Safari** on the menu followed by **Preferences**.
2. Click the **Security** tab.
3. Either check or uncheck the "Block pop-up windows" field.
4. To allow website exceptions use a supporting browser such as Chrome or Firefox.
5. Alternatively, **Shift + Command + K**.

Internet Explorer:

1. To the far right of the address bar click the gear icon.
2. Click **Internet Options**.
3. Select the **Privacy** tab and either check or uncheck the "Turn on Pop-up Blocker" field. Click **Apply**.

Edge:

1. To the far right of the address bar click the ellipsis.
2. Click **Settings**.
3. Under the Advanced Settings section click the "**View Advanced Settings**" button.
4. Use the **Block pop-ups** slider to make changes.

OPENING A PRIVATE BROWSING WINDOW

Chrome:

1. To the far right of the address bar click the ellipsis.
2. Click **New Incognito Window (Ctrl + Shift + N)**.
3. To end private browsing close the open window and click the ellipsis > **New Window (Ctrl + N)**.

Firefox:

1. Click the Open Menu icon to the far right of the address bar.
2. Click **New Private Window (Ctrl + Shift + P)**.
3. To end private browsing close the open window and click the Open Menu icon > **New Window (Ctrl + N)**.

Safari:

1. Click the **File** Menu, then click **New Private Window (Command + Shift + N)**.
2. To end private browsing close the open window and click **File > New Window (Command + N)**.

Internet Explorer:

1. To the far right of the address bar click the gear icon.
2. Click **Safety > InPrivate Browsing (Ctrl + Shift + P)**.
3. To end private browsing simply close the open window (**Ctrl + N**).

Edge:

1. To the far right of the address bar click the ellipsis.
2. Click **New InPrivate Window (Ctrl + Shift + P)**.
3. To end private browsing close the open window and click the ellipsis > **New Window (Ctrl + N)**.

[RESETTING BROWSERS](#)

In the event that common web browser troubleshooting is not helpful, a browser reset may be required. Please keep in mind that resetting the browser will revert all startup tabs, homepages, content settings, and all other customized preferences back to their installation defaults. It is recommended that the computer be restarted following any changes.

Chrome:

1. To the far right of the address bar click the ellipsis.
2. Click **Settings**
3. At the bottom of the **Settings** page click **Advanced**.
4. Under the Reset and clean up section click "**Restore settings to their original defaults.**"

Firefox:

1. To the far right of the address bar click the Open Menu icon.
2. Click **Help > Troubleshooting Information**.
3. In the top right of the newly opened window click the **Refresh Firefox** button and confirm the reset.

Safari:

1. Click **Safari** on the menu followed by **Preferences**.
2. Click the **Privacy** tab.
3. Click "**Remove All Website Data**" and select **Remove Now**.

Internet Explorer:

1. To the far right of the address bar click the gear icon.
2. Click **Internet Options**.
3. Select the Advanced tab and click **Reset** under Reset Internet Explorer settings.
4. Ensure that the **Delete personal settings** box is checked and click **Reset**.

Edge:

1. To the far right of the address bar click the ellipsis.
2. Click **Settings**.
3. Under the Clear browsing data section click the "**Choose what to clear**" button.
4. Ensure that all boxes are checked and click **Clear**.

Chrome:

1. To the far right of the address bar click the ellipsis.
2. Click **Settings**.
3. At the bottom of the **Settings** page click **Advanced**.
4. Under the Privacy and Security section click **Clear browsing data**.
5. Ensure that all desired check boxes are marked for deletion and click **Clear data**.
6. Alternatively, **Shift + Ctrl + Delete > Clear data**.

Firefox:

1. To the far right of the address bar click the Open Menu icon.
2. Click **Options**.
3. Click **Privacy & Security** from the menu and click **Clear data** and **Clear history** under their respective sections. Ensure that desired boxes are checked before clearing.

Safari:

1. Click **Safari** on the menu followed by **Preferences**.
2. Click the **Privacy** tab.
3. Click **Manage Website Data > Remove all**.
4. Alternatively, **Command + Option + E**.

Internet Explorer:

1. To the far right of the address bar click the gear icon.
2. Click **Internet Options**.
3. Select the **General** tab and click **Delete** under Browsing History. Ensure that the desired boxes are checked before deleting.
4. Click **Apply**.
5. Alternatively, **Ctrl + Shift + Delete**.

Edge:

1. To the far right of the address bar click the ellipsis.
2. Click **Settings**.
3. Click the **Choose What to Clear** button under Clear Browsing Data. Ensure that the desired boxes are checked before clearing.
4. Alternatively, **Ctrl + Shift + Delete**.

Training Guides & Information

Required Trainings

The following trainings are required for **all employees** and should be completed within 30 days of hire:

- FERPA
- Child Maltreatment
- Title IX
- Data Privacy and Security

Access these trainings through the Employee Learn Center in [Pack Portal](#) Contact [Cathy Naylor](#) (8079) for help and questions.

Most of our training content can now be found in the [Employee Learn Center](#).

General Training

The [Course Catalog](#) and [Find Learning](#) pages of the [Employee Learn Center](#) can direct you to the many courses available to you.

Other general training options for the campus are listed below. Many campus service areas are available for departmental trainings upon request.

Training Topic	Access/Contact	Additional Information
----------------	----------------	------------------------

Access and Institutional Engagement	Dr. Carlitta Moore	Introductory Video
Access and Accommodation Services	Dominique White	Introductory Video
Multicultural Affairs	Dr. Latika Johnson	Available for Departmental Trainings upon request
CPR Class	Spencer Bradley	Fees apply
Slow Moving Vehicle Safety	Learn Center	Required for all golf cart users

Recommended Training By Position

Click the contact name to let them know you plan to attend their scheduled training or to request a training session.

Administrative Specialist / Analyst and Fiscal Support positions may need some combination of the following trainings

Topic	Schedule	Location	Access/Contact
Banner Budget	Fourth Thursday of the month 9:00-12:00	Admin Building, Conference Room A	Janet Moore
Banner Finance			Learn Center - Banner and SSB9 Catalogs
Banner Student Module Training (Academic Units)	Every Wednesday 10:00 AM	Via Zoom	Jesse Blankenship
Banner Procurement (Guidelines, Requisitions, Receiving)	by request		Mike Smith / Learn Center
EPAF (Payroll, Electronic Personnel Action Form)	Second Thursday of the month 2:00 - 4:00	Admin Building, Conference Room A	Angela Gibson
P-Card Reconciliation (Concur)	by request		Mike Smith / Learn Center
Sponsored Program Accounting (Grants)	by request		Sponsored Programs

Taleo Admin Training (Hiring Process)	First Thursday of the month 3:00 - 4:00	Admin Building, Conference Room A	Kristin Carson
Travel (Concur)	by request		Billy Hogue / Learn Center

Faculty and Adjunct positions may need some combination of the following trainings:

Training Topic	Access/Contact
Banner Finance (If managing/approving a budget)	Learn Center - Banner and SSB9 Catalogs
Banner Student	Registrar's Office
Travel (Concur)	Billy Hogue / Learn Center
Sponsored Program Accounting (Grants)	Sponsored Programs
New Faculty Orientation	Learn Center
Faculty Professional Development and Training Guides	CETL

Facilities Management positions may need some combination of the following trainings:

Training Topic	Access/Contact
Fork Lift Safety	Learn Center
Slow Moving Vehicle Safety	Learn Center
Other Health/Safety Trainings	Learn Center

CONTACT TRAINING & DEVELOPMENT

[Cathy Naylor](#)

Phone: 870-680-8079