

Procedures

Browse approved IT procedures that provide step-by-step guidance for implementing policies and standards across the organization. These resources help ensure consistency, accountability, and the effective execution of operational and regulatory requirements.

- [3.1 Asset Management Procedure](#)
- [3.2 Canvas Live Course Access - Instructional Support Procedure](#)
- [3.3 Copyright Infringement Procedure](#)
- [3.4 Firewall Exceptions and Ruleset Procedure](#)
- [3.5 VPN Access Procedure](#)

3.1 Asset Management Procedure

Effective Date: March 4, 2025

Revised Date: March 31, 2025

1. Procurement of IT Assets

All IT assets (e.g., laptops, desktops, tablets) must follow the institutional procurement process. For details, refer to the [Technology Purchase Process](#).

2. Initial Setup and Configuration

Once received by Central Receiving, assets are transferred to ITS Hardware Technicians or Campus Technicians for initial setup, which includes:

- Installing the standard OS and required software.
 - Applying standardized configurations per A-State IT guidelines.
 - Adding departmental-specific software (as approved by IT Security).
 - Enabling endpoint protection, encryption, and other security settings.
 - Enrolling the device in the university's device management systems:
 - **KACE** (for Dell devices)
 - **Jamf** (for Apple devices)
-

3. Asset Registration in TeamDynamix (TDX)

Technicians must register each asset in TeamDynamix (TDX) with the following details:

- Owner
- Technician Responsible
- Status
- Asset Name
- Device Specifications / Item Description
- ITS Use Info (Serial Number, Model, Supplier, Warranty, MAC, IMEI, etc.)

This registration ensures accurate tracking, maintenance, and compliance.

4. Asset Tagging & Inventory by Property Accounting

After TDX entry:

- **Property Accounting** affixes the official asset tag.
- Departments should notify Property Accounting **before delivering devices** to the end user so tagging can occur on-site.

Contact: **James Riles** - jriles@astate.edu

Once tagged, the asset is:

- Added to the university asset database
- Updated in TDX with inventory confirmation and ownership

5. Asset Reallocation & Employee Termination

When an employee leaves or changes roles:

1. Submit the [Equipment Update Form](#).
2. IT Services or the department collects the asset.
3. Perform security checks:
 - Remove user credentials
 - Sanitize data per A-State policy
 - Reformat/reimage the device
4. Update TDX with reassignment or storage status

If a new asset is issued, the status of the previous one (e.g., reassigned, sent to M&R) must be reported to Property Accounting.

6. End-of-Life (EOL) & Disposal Process

When an asset is no longer viable:

1. Submit the [Excess Equipment Removal Form](#).
2. IT Services conducts the following:
 - Final security wipe
 - Remove & shred hard drives (if applicable)
 - iPads and other sealed devices are sent to Property Accounting for shredding
3. Update the asset's status in TDX:
 - Decommissioned
 - In storage (if awaiting M&R pickup)

Devices are processed through M&R or other approved disposal vendors.

7. Compliance and Security Review

A-State performs regular audits to ensure asset management compliance:

- **Annual Inventory Review** (by Property Accounting)
 - Every asset is physically verified on a three-year rotating cycle.
 - Interim years require verification by Dean/Director via updated asset reports.
- **Security Monitoring**
 - Assets are tracked via platforms like **Armis** for unusual network activity.

Any discrepancies, security risks, or policy violations are reported to:

- ITS
- Property Accounting
- UPD (if applicable)

Departments must also follow the [Property Accounting Manual](#) for full compliance.

3.2 Canvas Live Course Access - Instructional Support Procedure

Effective Date: February 28, 2026

Revised Date: August 11, 2026

1. Purpose

This procedure establishes the approved process for granting access to live Canvas course shells for instructional support personnel, including Graduate Assistants (GAs), Teaching Assistants (TAs), and Academic Assistants.

The objective is to ensure:

- Appropriate academic oversight
- FERPA compliance
- Proper role assignment aligned with instructional responsibilities
- Clear separation of grading authority, instructional record, and ability to edit content within the live Canvas shell
- Consistency between Banner, Coursedog, and Canvas role governance

2. Scope

This procedure applies to all live course shells within Canvas used for:

- Traditional (on campus) courses
- A-State Online (AOS) courses
- International campus courses (e.g., Qatar, Mexico)

This procedure applies only to instructional support access. It does not govern primary instructor assignments, which are managed through Banner and Coursedog.

3. Guiding Principles

- Access to live academic courses is restricted and role based.
- Grading authority must align with official Banner instructor-of-record designation.
- FERPA compliance must be verified prior to course enrollment.
- ITS does not override academic approval workflows.
- All access must follow documented request and approval processes.

4. Role Definitions and Access Levels

4.1 Graduate Assistant (No Grading Role)

Primary Use: Traditional courses

Canvas Role: GA/Tutor (No Grading)

Permissions:

- View course content
- Interact with students
- Assist with instructional support
- **No access** to gradebook grading functions

Approval & Enrollment Process:

1. Request submitted via approved online form. Individual **MUST** have completed FERPA training prior to requesting access.
2. Approval required from Registrar prior to ITS/Canvas action.
3. Upon receipt of approved request, ITS/Canvas:
 - Enrolls user in Canvas
 - Confirms completion of enrollment

4.2 Graduate Assistant (Requiring Grading Access)

Primary Use: Traditional courses

Canvas Role: Instructor (Must be Assigned in Banner/Coursedog)

Permissions:

- View/edit course content
- Interact with students
- Assist with instructional support
- Access to gradebook grading functions

Approval & Enrollment Process:

1. Request submitted to Registrar to have individual coded as instructor in Banner. Individual **MUST** have completed FERPA training prior to requesting access.
2. The GA must be added in Banner as a secondary or co-instructor, and this is processed through Coursedog.
3. Live sync between Coursedog, Banner, and Canvas will provide access to Canvas live shell within 24 hours.

4.3 Academic Assistant (AOS Courses – Instructional Connections)

Primary Use: A-State Online (AOS) courses

Canvas Role: TA

Permissions:

- View course content (no course content edit capabilities)
- Interact with students
- Assist with instructional support
- Access to gradebook grading functions
- The TA role cannot select the final grade for moderation or send final grades to Banner during final grading — this **MUST** be done by the primary instructor (or instructor(s) coded in Banner/Coursedog).

Pre-Requisites & Enrollment Process:

1. Sponsored account created through HR process: <https://kb.astate.edu/attachments/1236>
2. Individual **MUST** have completed FERPA training prior to being added to Canvas shell.
3. After prerequisites are verified, user is enrolled directly in Canvas by ITS/Canvas admins.

These users are not added to Banner as instructors of record.

4.4 Teaching Assistant (A-State Qatar)

Primary Use: A-State Qatar courses

Canvas Role: TA

Permissions:

- View course content (no course content edit capabilities)
- Interact with students
- Assist with instructional support
- Access to gradebook grading functions
- The TA role cannot select the final grade for moderation or send final grades to Banner during final grading — this **MUST** be done by the primary instructor (or instructor(s) coded in Banner/Coursedog).

Pre-Requisites & Enrollment Process:

1. Sponsored account created through HR process: <https://kb.astate.edu/attachments/1236>
2. Individual **MUST** have completed FERPA training prior to being added to Canvas shell.
3. After prerequisites are verified, user is enrolled directly in Canvas by ITS/Canvas admins.

These users are not added to Banner as instructors of record.

4.5 Access to Previous Term Live Course Shells

Primary Use: Instructors, Department Chairs, College Deans

Canvas Role: Instructor

Access to a previous term live Canvas course shell is restricted and requires formal approval due to FERPA, academic record integrity, and grading data considerations.

This section applies to any individual requesting access to a concluded live course shell:

- Instructors
- Department Chairs & College Deans

Approval & Request Process

Access to a previous term shell requires a formal email request to the Registrar (Tracy Finch – tfinch@astate.edu).

The request must include:

- Full name of the individual to be added
- A-State ID number of the individual
- Course CRN, term, and course information
- Justification for access

Registrar Review

The Registrar will:

1. Verify the individual's identity.
2. Confirm FERPA compliance.
3. Review and approve the access request.

If approved, the Registrar will send a formal request to: canvas@astate.edu

ITS/Canvas Admin Actions

Upon receipt of formal approval from the Registrar, ITS/Canvas Admin will:

- Enroll the approved individual in the specified Canvas course shell.
- Assign the appropriate role.
- Confirm completion of enrollment.

Important Notes

- ITS/Canvas Admin will not process requests for previous term access without formal Registrar approval.
- Direct instructor requests to ITS/Canvas Admin will be redirected to the Registrar.
- Role assignment must align with academic record and grading authority guidelines outlined in Sections 4.1–4.4.

4.6 External User Access (Sponsored Accounts)

Primary Use: External Reviewers, Accreditors, Auditors

Canvas Role: Observer, Accreditor/Auditor

External users who require access to Canvas for official university business (e.g., accreditation reviews, audits, or program evaluations) must be provisioned through a sponsored account process. These users are limited to access that supports their review function and are restricted to directory-level information only.

This section applies to any non-A-State affiliated individual requesting Canvas access:

- Accreditation reviewers
- External auditors
- Program evaluators or consultants

Approval & Request Process

1. Sponsored account created through HR process: <https://kb.astate.edu/attachments/1236>
2. Request submitted via approved online form.
3. Approval required from Registrar prior to ITS/Canvas action.
4. Upon receipt of approved request, ITS/Canvas:
 - Enrolls user in Canvas
 - Confirms completion of enrollment

These users are not added to Banner as instructors of record.

Important Notes

- External users provisioned under this section are not required to complete FERPA training.
- Sponsored accounts must be time-bound and reviewed periodically.
- Access will be removed automatically at the end of the approved period unless renewed.
- Sponsoring departments are responsible for ensuring appropriate use and notifying ITS when access is no longer required.

- Access is restricted to directory information only and must not include access to:
 - Grades
 - Submissions
 - Personally identifiable student information (beyond directory data)

4.7 Observer Access - Student Academic Support

Primary Use: Athletic Academic Advisors, Learning Community Staff, and Other Approved Student Support Personnel

Canvas Role: Observer

Observer access may be granted to designated university personnel who have a legitimate educational need to monitor and support student academic progress but who do not have instructional or grading responsibilities within the course.

Common uses of Observer access include:

- Athletic academic advisors supporting student-athletes
- Learning community advisors or coordinators supporting participating students
- Other university personnel with an approved academic support responsibility

For a detailed description of Canvas Observer visibility and participation, refer to Instructure's documentation:

<https://community.instructure.com/en/kb/articles/387091-observer-visibility-and-participation>

Approval & Request Process

Observer access must be based on a legitimate university academic-support function and must be formally approved by the Dean of University College, Dr. Nikesha Nesbitt (nnesbitt@astate.edu).

The request should identify:

- Full name and A-State ID of the individual requesting Observer access
- Department, program, or unit the individual represents
- Academic support function requiring access
- Student(s) or student population for whom access is required
- Requested duration of access, when applicable

Upon approval by the Dean of University College, the approved request will be forwarded to ITS/Canvas Admin for processing.

These users are not added to Banner as instructors of record.

Important Notes

- Observer access does not constitute instructor, teaching assistant, or grading authority.
- Observer access must be limited to students for whom the individual has an approved academic-support responsibility.
- Observer access must be removed when the individual's academic-support responsibility ends or the approved access is otherwise no longer required.
- ITS/Canvas Admin will not grant Observer access without documented approval from the Dean of University College.
- Observer access remains subject to applicable university policies, FERPA requirements, and the permissions and limitations configured for the Canvas Observer role.

5. Role Definitions and Access Levels

Registrar's Office

- Approves GA role assignments
- Approves grading authority requests
- Oversees Banner instructor designation

Academic Units / Instructors

- Determine level of access required
- Submit appropriate requests
- Ensure role justification aligns with instructional need

ITS/Canvas Admin

- Verifies approved documentation
- Enrolls users in Canvas when appropriate
- Ensures role accuracy

6. Procedure Review

This document will be reviewed and reaffirmed annually, or upon significant changes to university governance, systems, or regulatory requirements.

Effective Date: February 28, 2026

Next Review Date: February 28, 2027

Version: 1.0

3.3 Copyright Infringement Procedure

Effective Date: October 4, 2025

Revised Date: October 4, 2025

1. Purpose

This procedure establishes Arkansas State University's official process for responding to digital copyright infringement notices in compliance with the Digital Millennium Copyright Act (DMCA). It defines the steps ITS and Legal Counsel must take upon receipt of a notice, ensuring institutional compliance and protection under the DMCA's "safe harbor" provisions.

2. Scope

This procedure applies to all faculty, staff, students, and affiliated users of the Arkansas State University network and computing resources. It covers all forms of digital material, including video, audio, software, and written works distributed or stored through university systems or networks.

3. Background

The Digital Millennium Copyright Act (DMCA) establishes federal protection for copyrighted digital and electronic materials. Under the Act, copyright owners or their agents may submit infringement notices to Internet Service Providers (ISP's) alleging unauthorized distribution or use of protected content.

At Arkansas State University, copyright infringement notices are received by University Legal Counsel, which then coordinates with Information Technology Services (ITS) to identify and notify the alleged offender.

The University maintains a "safe harbor" from liability when it acts promptly to notify alleged infringers and remove or restrict access to infringing materials.

4. Standard Requirements

- All copyright infringement notices received by the University must be processed through Legal Counsel and ITS.
- ITS must investigate and resolve the notice within 24 hours of receipt by identifying the associated IP address, time stamp, and registered network user.

- Users found in violation will be notified in writing and provided instructions to remove or dispute the alleged content within ten (10) business days.
 - Users who fail to respond or remove the material within the specified timeframe will be considered in violation of the [A-State Appropriate Use Policy](#) and may face disciplinary action and/or legal consequences.
-

5. Copyright Infringement Notice Processing

The following steps outline how Arkansas State University processes copyright infringement notices under the DMCA:

1. **Receipt of Notice**

Copyright infringement notices are submitted electronically by plaintiffs (copyright owners or their agents) to a published email address managed by **University Legal Counsel** or **Information Technology Services (ITS)**.

2. **Identification of Offense**

Legal Counsel (if originally notified) forwards the notice to ITS for identification of associated user(s). ITS resolves the reported IP address and time stamp to identify the registered user of the university device or asset associated with the alleged infringement.

3. **Notification to User**

1. **For students:** ITS will notify the Vice Chancellor for Student Affairs/Dean of Students. A formal written notification to the alleged offender within 24 hours of receipt. See Appendix A for sample e-mail.
2. **For faculty and staff:** ITS or HR will issue a formal written notification to the alleged offender within 24 hours of receipt. See Appendix A for sample e-mail.
3. In all instances, the notification includes the copyrighted media title, IP address, and the time of the recorded infringement.

4. **Response Timeline**

The user has ten (10) business days to remove the copyrighted material or submit a counter-notification asserting that the use is protected under fair use, license, or another legal exemption.

5. **Enforcement**

1. **First Offense:** Written warning and educational notice from Student Affairs (or ITS).
 2. **Second Offense:** Immediate suspension of network and internet access until the matter is resolved through appropriate disciplinary channels as identified by Student Affairs (and HR where applicable for faculty/staff).
 3. **Repeated or Egregious Offenses:** May result in referral to Legal Counsel for further legal action (if applicable).
-

6. Compliance and Enforcement

Failure to respond to a copyright infringement notice may result in network suspension and referral for disciplinary or legal action. A-State maintains compliance with the DMCA and the A-State Appropriate Use Policy, ensuring the University's eligibility for safe harbor protection under federal

law. Continued violations may lead to permanent network access revocation or further institutional sanctions.

7. Standards Review

This document will be reviewed and reaffirmed annually, or upon significant changes to university IT governance, systems, or regulatory requirements.

Effective Date: October 4, 2025

Next Review Date: October 4, 2026

Version: 2.0

A-State maintains compliance with the DMCA and the A-State Appropriate Use Policy, ensuring the University's eligibility for safe harbor protection under federal law. Continued violations may lead to permanent network access revocation or further institutional sanctions.

Appendix A - Sample E-Mail to User

The following notice is provided to the accused from the University on the first offense.

Subject: Copyright Infringement Notice - Action Required

Dear Account Holder,

Arkansas State University has received notice of an alleged violation of the Digital Millennium Copyright Act (DMCA) by downloading protected materials, which has been traced back to your computer. A copy of the notice is enclosed at the bottom of this message.

Within ten (10) working days, you must respond to this email (with copy to CIO@AState.edu) by either:

1. Confirming that the offending materials have been removed from your computer; or
2. Filing a counter-notification asserting that your use of the identified materials does not violate copyright laws.

If you believe the factual allegation in the DMCA notice (e.g., that copyrighted materials were downloaded to your computer) is inaccurate, you must respond to this email (with copy to CIO@AState.edu) with an explanation of what facts you dispute and your basis for such dispute. Failure to respond to this notification within the prescribed time period will be treated as an admission of wrongful downloading in violation of the [Appropriate Use of Information & Technology Resources 3.05 - ASU System](#). Failure to respond, could subject you to legal action filed by the copyright owner.

A repeat offense will result in suspension of network access and referral for appropriate disciplinary action.

3.4 Firewall Exceptions and Ruleset Procedure

Effective Date: October 27, 2025

Revised Date: July 28, 2026

1. Purpose

This document establishes a standardized procedure for the firewall exceptions and rulesets on the Arkansas State University - Jonesboro (A-State) campus. The goal is to create a clear and consistent procedure for all firewall requests.

2. Scope

These procedures apply to all Arkansas State University - Jonesboro faculty and staff firewall requests.

3. Definitions

- **Firewall** - Network security device that monitors and controls incoming and outgoing traffic on the network based on predetermined rules.
 - **Ruleset** - A collection of rules that act as a security policy to filter network traffic.
 - **Port** - A communication endpoint that identifies a specific process or service on a device.
-

4. Firewall Exception Process

Firewall exceptions added to the A-State firewall must adhere to the following:

- Firewall exceptions (open ports) must be requested in writing via a TDX work order using the [Firewall Policy Change](#) form.
 - Requests must be justified and approved by the Security Division and the Networking Division.
 - Requests must be reapproved annually.
 - ITS may scan devices that can be accessed via open ports for security issues. All issues found must be corrected/justified in five business days or the firewall exception will be closed.
 - ITS may close an open port at any time for security reasons.
 - ITS may, at its discretion, decline to open a port.
-

5. Standards Review

This document will be reviewed and reaffirmed annually, or upon significant changes to university IT governance, systems, or regulatory requirements.

Effective Date: October 27, 2025

Next Review Date: July 28, 2027

Version: 1.1

3.5 VPN Access Procedure

Effective Date: October 27, 2025

Revised Date: October 27, 2025

1. Purpose

This document establishes a standardized guideline for remote access to Arkansas State University - Jonesboro (A-State) Virtual Private Network (VPN).

2. Scope

These guidelines apply to all employees, students and all authorized third parties (contractors or consultants) that will utilize VPN to access the A-State Network.

3. Definitions

- **VPN** – A Virtual Private Network that establishes a secure connection between two trusted locations (your computer and the A-State network) via an insecure, public network (the Internet).
 - **Geo Blocked** – Restricting access to the network by the user's geographic location.
-

4. Guidelines

VPN access allows users unrestricted access to the Arkansas State University computer network from locations external to the Jonesboro campus. This unrestricted access to the network could increase the University's exposure to viruses, malware, and could allow hackers using compromised accounts greater access to the A-State network. These guidelines should be followed to lessen the security risk of the campus at large.

- Standard VPN access will be approved by the Security Division if Chair/Dean/Dept. Head approval is not available. If Chair/Dean/Dept. Head approval is available, then VPN access will be granted without further approval from ITS.
 - **Service:** [A-State VPN Access Request](#)
- VPN access is geo-blocked to the United States and Canada.
- International VPN access is permitted on a per-user and per-country basis. This requires a separate set of approvals as well as standard VPN access. This access must be approved by the Security Division and the Networking Division.
 - **Service:** [International VPN Access Request](#)

- Devices failing security scans may be denied VPN access.
 - Access may be suspended/terminated by ITS at any time if access could cause a security issue.
 - VPN access is logged, and the logs will be retained for one year.
 - Logging includes:
 - Connection/disconnection times
 - IP address received from DHCP
 - Connecting IP address
 - IP address(es) accessed
 - Username that opened the connection
 - ITS may require devices connecting via VPN to be scanned for up-to-date OS and software patches and/or versions, current antivirus software, or other security related issues.
 - 3rd party vendors may apply for VPN access but require a sponsored A-State user account.
-

5. Approved VPN Clients

To ensure secure and supported remote connectivity to the A-State network, only University-approved Virtual Private Network (VPN) client software may be used to establish VPN connections. Use of unsupported or unauthorized VPN clients is prohibited.

The following VPN clients are approved for use on A-State managed and personal devices when connecting to the University network:

- **GlobalProtect VPN (Palo Alto)** - This client is the primary supported VPN solution for faculty, staff, and authorized contractors requiring secure access to A-State resources. Instructions for obtaining, installing, configuring, and using GlobalProtect are maintained by IT Services and available here: [How to Download VPN](#)
- **FortiClient VPN (Fortinet)** - The FortiClient VPN client is approved for use where GlobalProtect is unavailable or not appropriate (primarily for mobile VPN use). FortiClient may be required for access to specific systems, departments, or research environments that depend on Fortinet VPN infrastructure.
- **Extreme ZTNA (Extreme Networks) [LIMITED USE WITH ITS APPROVAL]** - A-State is implementing Extreme ZTNA to provide identity-based, "least-privilege" access to specific University applications. This solution may be required for access to certain high-security systems or cloud-based resources. During the current implementation phase, its use is restricted to authorized testing groups and specific departmental workflows as directed by IT Services.

Requirements & Restrictions

Approved VPN clients must be obtained directly from official University distribution points or the respective vendor's official repositories. **The above VPN clients are the only approved platforms to be used to connect to the A-State network unless otherwise authorized by Information Technology Services.**

VPN clients must be kept up to date with the latest security patches and versions supported by A-State Information Technology Services.

Use of third-party VPN technologies/clients not explicitly approved in this section is not permitted and may result in loss of VPN privileges and further institutional sanctions.

6. Standards Review

This document will be reviewed and reaffirmed annually, or upon significant changes to university IT governance, systems, or regulatory requirements.

Effective Date: October 27, 2025

Next Review Date: October 27, 2026

Version: 1.1