2.2 Business Continuity and Disaster Recovery Standard

Effective Date: July 1, 2026
Revised Date: July 1, 2026

1. Purpose

This Standard establishes the mechanisms necessary to ensure Arkansas State University (A-State) can maintain or rapidly resume essential academic, administrative, and technology operations following a disruptive incident. This standard aligns institutional service criticality with technical restoration priorities, establishes recovery time objectives (RTO) and recovery point objectives (RPO) expectations, and defines governance, testing, communication, and compliance requirements for ITS.

2. Scope

This standard applies to all Arkansas State University Information Technology Services (ITS)-supported environments, services, and technology resources, including enterprise systems and services such as compute, storage, operating systems, databases, software, and technical documentation; enterprise communications encompassing network infrastructure, VoIP, email, web presence, and ISP or carrier services; ERP application data, including Banner ERP and related systems; and data center facilities, specifically the primary ITS Data Center, as well as cloud-hosted services with verified disaster recovery capabilities.

3. Definitions

Technology Resources – The machines, devices, systems, services, and related components used in information processing. This includes:

- Machines, devices, and transmission facilities used in information processing, such as computers, word processors, terminals, telephones, cables, software, and related products.
- Devices used to process information through electronic capture, collection, storage, manipulation, transmission, retrieval, and presentation of information in the form of data, text, voice, or image, including telecommunications and office-automation functions.
- Any component related to information processing and wired or wireless telecommunications, including hardware, software, services, planning, personnel, facilities, and training.
- Procedures, equipment, and software designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, along with associated personnel such as consultants and contractors.

- All email accounts issued by the Arkansas State University System.

User – Any individual, whether authorized or unauthorized, who makes use of any university technology resource from any location. This includes faculty, staff, students, contractors, affiliates, and members of the system community.

System Community - Any person who accesses the ASU System's IT infrastructure who is not classified as a member of the faculty, staff, or enrolled student.

Systems Authority - ASU System delegates oversight of particular systems to the head of a specific unit of the ASU System or to an individual faculty member, in the case of technology resources purchased with research or other funds for which he or she is personally responsible.

Systems Administrator - A Systems Authority may designate another person as "Systems Administrator" to manage the particular system assigned to him or her. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular technology resources.

Certifying Authority - This is the Systems Administrator or other ASU System authority who certifies the appropriateness of an official ASU System document for electronic publication in the course of ASU System business.

Specific Authorization - This means documented permission provided by the applicable Systems Administrator.

4. Responsibilities

All university personnel involved in the configuration, maintenance, and review of controls necessary to ensure the effective management and remediation of technology resource vulnerabilities. This includes:

Chief Information Officer (CIO) - Responsible for the executive sponsorship, governance, and oversight of the University's business continuity and disaster recovery processes within the scope of this standard. Ensures that applicable regulatory, statutory, and contractual obligations are identified, translated into actionable controls, and operationalized across institutional systems and processes.

Assistant Vice Chancellor of IT Infrastructure and Operations – Responsible for the planning, execution, and continuous improvement of the University's Business Continuity and Disaster Recovery (BC/DR) program. Oversees all infrastructure-related recovery capabilities, including systems, network, endpoint, and IT support services. Leads incident response and recovery operations for infrastructure services and ensures all ITS teams are aligned with and operating in accordance with this standard.

Assistant Vice Chancellor for ERP Application Services – Accountable for the continuity, recovery, and integrity of the University's Enterprise Resource Planning (ERP) systems and associated data. Leads ERP-specific recovery planning, testing, and execution. Coordinates with the

Assistant Vice Chancellor of IT Infrastructure and Operations during incidents to ensure infrastructure and application recovery efforts are aligned, and ERP services are restored in accordance with defined recovery objectives.

Director of IT Security – Responsible for overseeing the university's IT security program and serves as a member of the Crisis Assessment and Management Team during incident response activities. Works closely alongside the AVC of IT Infrastructure and Operations when incidents are classified as a security incident.

Crisis Assessment and Management Team (CAMT) - Responsible for evaluating incidents, assigning crisis classification, authorizing plan activation, and providing executive updates. This team consists of the CIO as Lead, Director of IT Security, Assistant Vice Chancellor of IT Infrastructure and Operations, Assistant Vice Chancellor for ERP Application Services, and the directors for IT Support, Systems, and Networking.

Crisis Recovery Team (CRT) - Responsible for executing system, application, network, communication, and data restoration activities according to the mapped prioritization and runbooks.

Executive Leadership – Responsible for authorizing major institutional actions, including alternate facilities and public communications. This consists of the Chancellor, CFO/VCFA, Provost, and other senior leaders as necessary.

5. Standard Exceptions

The Chief Information Officer is authorized to review and approve exceptions to this standard when organizational needs justify a deviation, and the associated risks are deemed acceptable. All exceptions must be documented, including a defined scope, a scheduled review date, and compensating controls when appropriate. The CIO may delegate this authority as necessary but retains overall accountability for exception management and review.

6. Incident Classification

The following matrix outlines how incidents and disasters will be categorized by the Crisis Assessment and Management Team (CAMT).

Category	Description	Key Determinants
1	Minor disruption to non-critical systems	Expected resolution < 24 hours; no alternate site needed
2	Major disruption; recovery at primary site > 24 hours but feasible	Damage or facility issue; primary data center still usable
3	Total outage of multiple systems; alternate site faster	Major facility disruption; extensive damage; recovery > 72 hours
4	Total loss of data center; recovery time unknown	Data center destroyed or unsafe; full relocation required

7. Service Criticality and Restoration Alignment

A-State ITS aligns institutional CAMT incident classifications with ITS technical restoration priorities to ensure a unified, risk-based recovery sequence.

Institutional Criticality Category Alignment

Category	Description	Example Functions
1 – Critical (Immediate)	Essential to life safety, financial integrity, core academic operations, and communications.	Receiving funds, student registration and grading, transcript production, VoIP, email, and web presence.
2 – Priority (24–72 hours)	Important; delays beyond 24–72 hours significantly affect operations or compliance.	Procurement and disbursement, admissions processing, student account changes, and ISIR loads.
3 – Important (72+ hours)	Tolerates longer outages without major institutional risk.	HR and Financial Aid tasks, Alumni/Development, and lower-impact departmental operations.
4 – Non-Critical	Minimal impact; restore after Categories 1–3.	Departmental servers and low-impact web or class servers.

Note: Criticality may vary at significant times on the university calendar, including the first week of a semester, final exam week, or fiscal year end.

Mapping to Technical Restoration Priorities

ITS Priority	Mapped Institutional Category	Examples from Inventory
Priority 1	Category 1	Active Directory, DNS forwarders, VMware clusters, SAN management, VoIP Call Managers, E911, Exchange CAS/Mailbox, and Banner integrations.
Priority 2	Category 2	ISI Billing, Campus Receivables Collector, Ethos production, Banner XE Solutions Manager, and Doc-Image.
Priority 3	Category 3	CommServ/Syslog, wireless controllers, test environments, and secondary AD/DC nodes.
Priority 4	Category 4	Departmental servers, Mailman, KACE client management, and VDI non-essential components.

The full restoration inventory with system owners and contacts is maintained in the **Restoration Priorities** register, IRP Appendix B. During an event, CRT restores Priority 1 systems first, followed by Priorities 2–4.

Unless otherwise specified in system-specific runbooks, the following target ranges apply:

Recovery Objectives (RTO/RPO)

Category / Priority	Target RTO	Target RPO	Notes
1 / 1	Immediate to 4 hours	≤ 1 hour, or last successful transaction	Life safety and campus-wide communications take precedence.
2 / 2	≤ 72 hours	≤ 4 hours	Sequence ordered by academic and fiscal calendars.
3 / 3	≤ 7 days	≤ 24 hours	Supports rebuild and service hardening activities.
4 / 4	> 7 days, as scheduled	≤ weekly	Planned reintroduction after stabilization.

8. Infrastructure Redundancies and Failover

Arkansas State University maintains infrastructure redundancy and failover capabilities to support business continuity and disaster recovery objectives and to minimize the impact of infrastructure disruptions. The campus network is designed with dual cores to increase redundancy and sustain availability during incidents or periods of peak demand.

Critical enterprise services, including ERP, email, identity management, and backup infrastructure, are hosted in resilient cloud environments when available to leverage geographic redundancy and provider-managed failover. Voice and essential communications systems incorporate failover and survivability capabilities to maintain emergency and operational communications during outages.

Where defined by system criticality, contingency compute environments in Azure and Logical Front are available to support service restoration and continuity during prolonged disruptions. Infrastructure redundancy and recovery capabilities are reviewed and tested as part of ongoing BC/DR governance.

9. Backups and Data Protections

A-State implements layered backup and data protection mechanisms for critical infrastructure to support timely restoration following incidents or disruptions. Backup strategies are designed to align with defined recovery objectives and to reduce reliance on single locations, platforms, or technologies.

Standard backup processes, configurations, and retention expectations are documented and maintained in A-State ITS Backup Procedures, which are reviewed and updated annually to reflect current operational practices.

- Short-term on-premises backups for virtual machines and network-attached storage supporting rapid restoration needs. Currently implemented using a seven-day on-premises virtual machine and NAS backup model.
- Immutable offsite backup copies retained for a defined period to protect against data corruption, ransomware, or other destructive events. Currently implemented using a fourteen-day immutable offsite backup solution, such as Wasabi.

- Additional cloud-based backup replicas, maintained where configured, to enhance resiliency and geographic separation. Currently implemented through secondary cloud backup copies, such as Apex3.
- Data migration to institutionally approved cloud collaboration and storage services, where appropriate, to reduce dependency on on-premises storage infrastructure. Currently implemented through migration of NAS data to cloud-based collaboration platforms, such as Microsoft Teams and SharePoint.

Backup configurations represent baseline practices and may vary by system based on data classification, system criticality, architectural design, and risk considerations. Backup integrity and recoverability are validated through restoration testing as part of ongoing Business Continuity and Disaster Recovery governance. This restoration testing is completed in alignment with the testing and training cadence matrix.

10. Cloud Service Considerations

ITS leverages managed and cloud-hosted services to enhance resilience, availability, and disaster recovery capabilities. Critical institutional platforms are delivered through externally hosted software-as-a-service, platform-as-a-service, and infrastructure-as-a-service solutions that provide geographically distributed infrastructure, provider-managed redundancy, and documented disaster recovery capabilities.

11. Restoration Sequence

During an incident, the CRT executes restoration in the following order:

1. **Protect life safety and communication:** Restore VoIP/Call Managers, E911, Active Directory, DNS, email, core virtualization/storage, and essential Banner integrations.
2. **Stabilize academic and financial operations:** Restore Priority 2 systems aligned to the calendar, including procurement, disbursement, admissions/registrar, Campus Receivables, Doc-Image, and Ethos production.
3. **Resume supporting functions:** Restore Priority 3 systems, including secondary AD/DCs, Syslog, wireless, and test environments.
4. **Restore low-impact and departmental resources:** Restore Priority 4 systems, including departmental servers, VDI non-critical components, Mailman, and KACE.

12. Communication

Internal Communication

- Activate the Calling Tree as required based on incident scope and severity.
- Utilize available communication channels, including hotline or voicemail broadcasts, Microsoft Teams, email, and campus web updates.
- Provide status updates to executive leadership and key stakeholders at regular intervals appropriate to the severity and operational impact of the incident, as determined by the Crisis Assessment and Management Team.

External Communication

External communications during incidents will be managed in accordance with the A-State Campus Emergency Action Plan and established institutional processes.

- University Police coordinate emergency response and engagement with external emergency services as required.
- The Office of University Communications serves as the sole authorized point of contact for public statements and media communications.
- Executive leadership is responsible for notifications to external agencies, insurers, regulatory bodies, and institutional partners as applicable.

External communications priorities, timing, and messaging will guide and inform corresponding internal communications to maintain alignment, accuracy, and institutional control during incident response and recovery.

13. Testing, Training, Exercise, and Review

Arkansas State University Information Technology Services maintains a structured and recurring program of testing, training, exercise, and review to validate the effectiveness of business continuity and disaster recovery capabilities.

The following activities are conducted according to the established cadence below, with additional testing performed as warranted by system changes, risk assessments, or significant incidents:

Annual Activities

- Business Continuity and Disaster Recovery tabletop exercises are conducted annually to validate roles, decision-making authority, escalation paths, and internal and external communication coordination.
- Comprehensive After-Action Reviews are completed following annual exercises and any declared major incidents to document lessons learned, identify gaps, and develop corrective action plans. Corrective actions are tracked to completion.

Periodic Technical Testing

- Targeted technical recovery tests for critical enterprise systems, communications infrastructure, ERP data, and cloud-hosted services are conducted on a recurring basis, not less than annually, and may be scheduled more frequently for systems classified as Critical or Priority.
- Backup restoration drills are performed quarterly to validate data recoverability, backup integrity, immutability protections, and alignment with defined RTO and RPO targets.
- Ad-hoc testing may be initiated following major infrastructure changes, migrations, or onboarding of new critical services.

The results of all exercises and tests will be documented and reviewed by the CAMT, with the gap analysis generated from this review being used to improve business continuity and disaster

recovery readiness.

Testing and Training Cadence

Activity	Minimum Requirement	Recommended Requirement	Responsible Party
BC/DR Specific Tabletop Exercise	Annually	Semiannually	Assistant Vice Chancellor of IT Infrastructure and Operations
Backup Restoration Drills - Active Test, Non-ERP	Quarterly	Monthly	Assistant Vice Chancellor of IT Infrastructure and Operations
Backup Restoration Drills - Active Test, ERP	Quarterly	Monthly	Assistant Vice Chancellor of ERP Application Services
Documentation Review	Annually	Semiannually	Assistant Vice Chancellor of IT Infrastructure and Operations

14. Security and Compliance Alignment

Business Continuity and Disaster Recovery planning, execution, and testing activities must align with institutional information security standards and applicable legal, regulatory, and contractual requirements. This includes, but is not limited to, requirements related to criminal justice information, federal financial aid regulations, data protection, and records retention.

Information security controls must remain effective during backup, recovery, alternate processing, and restoration activities to protect the confidentiality, integrity, and availability of institutional data.

15. Monitoring and Enforcement

The Assistant Vice Chancellor of IT Infrastructure and Operations is responsible for monitoring compliance with this Business Continuity and Disaster Recovery Standard across ITS-supported systems and services.

Compliance is assessed through a combination of:

- Annual BC/DR plan reviews and tabletop exercises
- Scheduled technical recovery and restoration testing
- Backup and restore validation activities
- After-Action Reviews following incidents or exercises
- Periodic audits or assessments requested by executive leadership, Internal Audit, or regulatory bodies

The Assistant Vice Chancellor of IT Infrastructure and Operations is responsible for ensuring that systems managed under their purview meet defined recovery objectives, responsible team members participate in required testing, and accurate recovery documentation is regularly

maintained.

Identified gaps, deficiencies, or failures to meet defined BC/DR requirements must be documented and tracked through corrective action plans with assigned owners and target remediation dates. Risks that cannot be remediated within acceptable timeframes must be formally documented and escalated to the CIO.

16. Standards Review

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

Effective Date: July 1, 2026
Next Review Date: July 1, 2027
Version: 1.0

Referenced Policies, Standards, and Procedures

- Technology Resource Management Standard
- Information Technology Services (ITS) Communication & Service Level Agreement (SLA) Standards
- Data Security and Classification Policy
- A-State Campus Emergency Action Plan
- A-State ITS Backup Procedure

Revision #3
Created 2026-06-26 01:35:59 UTC by Christopher Boothman
Updated 2026-06-26 01:43:27 UTC by Christopher Boothman