UNIVERSITY OF NORTH ALABAMA // OFFICE OF INFORMATION TECHNOLOGY

WEB TEAM CONTINUITY & CONTINGENCY PLAN

// OPERATIONAL RISK, SUCCESSION, INCIDENT RESPONSE & KNOWLEDGE TRANSFER //

DATE: March 2026 VERSION: v1.0 // Living Document

// CONTENTS

01 PURPOSE & SCOPE

This document consolidates continuity and contingency protocols for the Web Development team within the Office of Information Technology. It addresses four distinct risk categories:

- **Staff turnover and succession** — ensuring institutional knowledge is not lost when personnel change
- **System outages and disaster recovery** — defining response procedures for critical platform failures
- **Budget or organizational disruption** — outlining response strategies for resource or structural changes
- **Institutional compliance** — providing documentation sufficient for HR, audit, and accreditation review

This plan covers all systems and platforms owned or operated by the Web Development team and applies to all current team members.

02 TEAM STRUCTURE

Role	Name	Responsibilities

Role	Name	Responsibilities
Team Lead	Heath Matlock	Technical leadership, architecture decisions, platform administration, institutional relationships
Web Developer I	Bobby Martin	Application development
Web Developer I	Tony Bush	Application development, Slate integration specialist
Web Developer III	(third developer)	Application development

03 SYSTEMS INVENTORY & CRITICALITY

CRITICALITY DEFINITIONS

- **Critical** — Failure directly disrupts institutional operations or public-facing services
- **High** — Failure significantly degrades team productivity or cross-team coordination
- **Medium** — Failure affects specific workflows but does not disrupt primary operations
- **Low** — Failure has minimal operational impact; restoration can be scheduled

RECOVERY PRIORITY DEFINITIONS

- **P1** — Restore within 4 business hours; active response required immediately
- **P2** — Restore within 1 business day; response begins within 4 hours

System	Description	Criticality	Primary Administrator	Priority
una.edu	Primary institutional website (Cascade CMS)	Critical	Team Lead	P1
apps.una.edu	WordPress via CloudPanel on unasites.com (American Cloud)	Critical	Team Lead	P1
1Password	Team credential and secrets management	Critical	Team Lead (secondary: Lee)	P1
Microsoft Entra SSO	SSO for internally developed applications	High	Team Lead	P1
Slate integrations	Admissions CRM integrations; affects enrollment workflows	High	Tony Bush / Team Lead	P1
Slack	Team communication; #alerts channel for monitoring	High	Team Lead (secondary: Lee)	—
GitHub	Source code repository	High	Tony Bush, Bobby Martin (owners)	—

System	Description	Criticality	Primary Administrator	Priority
una.edu Database	MySQL; primarily supports Open Alabama reports	Medium	All (via 1Password)	—
Banner integrations	Campus directory integrations; code in team repository	Medium	Tony Bush, Bobby Martin, Team Lead	P2
Claude	AI assistant	Medium	Team Lead (Tony Bush, Bobby Martin: pending)	—
smallbusinessadvocate.una.edu	Third-party hosted application	Low	Team Lead	P2

04 KNOWLEDGE CONCENTRATION RISK

The following areas represent current gaps in documentation or coverage:

- **DNS access** — DNS is managed exclusively by the CIO. The Web Team has no DNS access and cannot resolve DNS-related outages independently. A defined, supervised change pathway would ensure recovery does not depend on a single contact.
- **Vendor relationships** — TAM and customer success manager contacts for Beacon are not yet documented. Primary contact for WPEngine/5by5 is not yet established.
- **Banner integration configurations** — Code is in the team repository but lacks documentation for independent troubleshooting or hand-off.
- **Slate integration configurations** — Tony Bush is primary specialist; configuration and dependency documentation is incomplete.
- **Backup procedures** — No formal backup process exists for the una.edu MySQL database. Current backups exist only on the Team Lead's machine.
- **apps.una.edu failover** — No failover strategy currently exists. A plan is in development for the new site, likely hosted on WPEngine.
- **unasites.com and American Cloud services** — Recovery procedures for apps.una.edu hosting environment are not documented.
- **smallbusinessadvocate.una.edu** — No documented response procedure or escalation path exists.

05 SUCCESSION & COVERAGE PROTOCOLS

5.1 PLANNED ABSENCE (VACATION, LEAVE)

Prior to any planned absence exceeding three business days, the Team Lead will:

01 Identify a temporary point of contact from the developer team

02 Brief that developer on any time-sensitive in-flight work

03 Ensure emergency credential access procedures (Section 8) are confirmed active

04 Notify the ERP Manager of the coverage arrangement

5.2 UNPLANNED ABSENCE (SHORT-TERM)

For unplanned absences expected to be fewer than five business days:

01 The available senior developer assumes day-to-day ticket and support queue management

02 Development and deployments continue normally

03 Emergency access to credentials is available via the procedure in Section 8

5.3 ACADEMIC BREAK & HOLIDAY COVERAGE

During extended academic breaks, the team follows a structured on-call approach to ensure systems are monitored without requiring everyone to remain available.

PRE-BREAK CHECKLIST

- Confirm all monitored systems are stable; review #alerts for any unresolved issues
- Verify uptime monitoring is active for apps.una.edu and smallbusinessadvocate.una.edu
- Ensure no deployments or pending updates are scheduled during the break period
- Confirm the on-call designee has access to all credentials needed for first-response recovery

ON-CALL ROTATION

- One team member is designated as the primary on-call responder for each break period
- Responsibility rotates across the team across the academic year
- The on-call designee must be reachable and able to respond within a reasonable window

RESPONSE EXPECTATIONS DURING BREAKS

- Response times are longer than normal business hours — expected and acceptable
- **Requires prompt attention:** una.edu or apps.una.edu is down; a P1 system is unreachable
- **Can wait until return:** minor display issues, non-critical requests, low-priority alerts

ESCALATION DURING BREAKS

01 On-call designee attempts first-response recovery

02 If unresolved, escalate to Team Lead

03 If Team Lead is also unreachable, escalate to ERP Manager

5.4 RISK: LOSS OF A DEVELOPER

IMMEDIATE RESPONSE (0–30 DAYS)

- Redistribute ticket queue across remaining developers, prioritizing compliance-critical issues
- Team Lead assumes additional development capacity for active projects

- Document all in-flight work before any departure

SHORT-TERM (30–90 DAYS)

- Begin posting for a replacement; leverage UNA CS program for student worker bridge capacity
- Evaluate which active projects can be deferred vs. those requiring external contractor engagement

MITIGATION (ONGOING)

- Maintain living documentation for all active projects, integrations, and credentials
- Cross-train developers on critical systems (Slate integrations, deployment workflows)
- No single developer should be the sole owner of any production system

5.5 EXTENDED OR PERMANENT DEPARTURE / LOSS OF TEAM LEAD

IMMEDIATE RESPONSE (0–30 DAYS)

- ERP Manager assumes interim oversight
- Senior developer steps into lead capacity for daily operations and ticket triage
- Active projects should be documented and hand-off-ready within 72 hours

SHORT-TERM (30–90 DAYS)

- ERP Manager initiates search for replacement or evaluates internal promotion pathway
- Team continues in maintenance mode, deferring new initiatives until leadership is stabilized
- Vendor and integration contacts accessible to ERP Manager

MITIGATION (ONGOING)

- Maintain a Team Lead operational runbook covering system architecture, vendor contacts, and active project statuses
- Ensure secondary 1Password admin (Lee) has documented access to all critical credentials

06 BUDGET CUTS OR ORGANIZATIONAL RESTRUCTURING

SCENARIO A: ONE POSITION ELIMINATED

- Consolidate to two developers; Team Lead increases direct development contribution
- Defer new application development; focus on WCAG compliance, una.edu maintenance, and existing platform obligations
- Engage UNA CS department for paid student worker support as a cost-effective bridge

SCENARIO B: TEAM DISSOLVED OR MERGED

- Document all institutional knowledge: credentials, integrations (Banner, Slate, Microsoft Entra), deployment environments, and active contracts
- Advocate to ERP Manager for retaining at minimum one technical FTE to manage una.edu and

contractual obligations

SCENARIO C: BUDGET FREEZE, NO REDUCTIONS

- Pause discretionary tool and platform spend
- Prioritize: WCAG compliance (regulatory/legal exposure) and production stability
- Defer: new application development and non-critical redesign work

MITIGATION (ONGOING)

- Maintain clear ROI documentation for team initiatives (cost avoidance, compliance risk reduction, enrollment-facing impact)
- Tie team value to institutional strategic priorities: enrollment, compliance, and operational efficiency

07 INCIDENT RESPONSE & DISASTER RECOVERY

7.1 UNA.EDU OUTAGE

una.edu runs on Cascade CMS. Bobby Martin and Tony Bush have access via 1Password.

Scenario	First Response	Escalation
Cascade CMS unavailable	Check Cascade hosting status; contact vendor	Team Lead > ERP Manager > Cascade support
Database failure	Restore from most recent backup	Team Lead > ERP Manager
DNS or network issue	DNS is outside Web Team scope — contact CIO directly. The Web Team has no DNS access.	Team Lead > CIO
Compromised credentials	Rotate via 1Password; audit access logs	Team Lead > ERP Manager

RTO: una.edu restoration targeted within 4 business hours for any outage.

! ACTION REQUIRED
No documented backup process exists for the una.edu MySQL database, which stores Open Alabama report data. Current backups exist only on the Team Lead's machine. An off-site backup process with documented restoration procedures should be established.

7.2 APPS.UNA.EDU OUTAGE

apps.una.edu is a WordPress site hosted via CloudPanel on unasites.com, running on American Cloud infrastructure. Credentials for American Cloud and CloudPanel are in 1Password.

Note: No failover strategy currently exists for apps.una.edu. A failover plan is in development for the new site, which will likely be hosted on WPEngine.

When the una.edu redesign launches, WPEngine (with 5by5 support) will serve as the hosting provider for all WordPress sites and response procedures will be updated accordingly.

Scenario	First Response	Escalation
WordPress CMS unavailable	Check unasites.com availability; verify American Cloud service status	Team Lead > American Cloud support
Database failure	Restore from most recent database backup	Team Lead > ERP Manager
SSO integration failure	No documented procedure — see action item below	Team Lead
Full platform unavailability	Restore from backup; notify affected departments	Team Lead > ERP Manager

! ACTION REQUIRED
No documented procedure exists for SSO/Entra integration failure on this WordPress site. A runbook for this scenario is a required action item.

! ACTION REQUIRED
No documented backup process or off-site backup exists for this environment. The database and unasites.com services are not sufficiently documented for independent recovery.

7.3 SMALLBUSINESSADVOCATE.UNA.EDU OUTAGE

smallbusinessadvocate.una.edu is a third-party hosted application. Uptime monitoring is active; alerts are delivered to the #alerts Slack channel.

! ACTION REQUIRED
No documented response procedure exists for this application. Contact information for the third-party host and a defined escalation path must be documented before this plan is operational.

7.4 MONITORING

Uptime monitoring is active for the following systems; alerts are delivered to the #alerts Slack channel:

- apps.una.edu
- smallbusinessadvocate.una.edu

7.5 SSO / MICROSOFT ENTRA OUTAGE

Scenario	First Response	Escalation
Microsoft-side outage	Check Microsoft service health dashboard; communicate status to affected users	Monitor Microsoft status; no internal action required
Configuration-level issue	Team Lead engages IT support and Entra admin console	Team Lead > ERP Manager

! ACTION REQUIRED
No documented procedure exists for configuration-level Entra failures affecting WordPress SSO. This must be addressed.

MITIGATION

- Document all registered applications and their redirect URIs
- Maintain break-glass accounts for critical systems where technically feasible

7.6 DATA LOSS EVENT

01 Immediately suspend write access to the affected system to prevent further data corruption

02 Notify ERP Manager within 1 hour of confirmed data loss

03 Engage backup restoration process; assess scope of loss against last clean backup

MITIGATION TARGETS

- Backup retention policy (target): daily for 30 days, weekly for 6 months
- Backups tested quarterly via restoration drill
- No production data stored exclusively in a single environment

08 CREDENTIAL & ACCESS MANAGEMENT

8.1 CREDENTIAL COVERAGE MATRIX

System	Current Admin	Secondary Admin	Emergency Access
una.edu (Cascade)	Bobby Martin, Tony Bush	— via 1Password	Partial
una.edu Database	All team members (via 1Password)	—	No
apps.una.edu / CloudPanel	Team Lead	— credentials in 1Password	No
American Cloud	All team members (via 1Password)	—	Yes

System	Current Admin	Secondary Admin	Emergency Access
Microsoft Entra (SSO)	Team Lead	—	No
1Password	Team Lead	Lee	Yes
Slack Workspace	Team Lead	Lee	Partial
GitHub	Tony Bush, Bobby Martin (owners)	—	Yes
Claude	Team Lead	Pending (Tony Bush, Bobby Martin)	No

! ACTION REQUIRED
All rows in this table should have a designated secondary admin and documented emergency access before this plan is considered operational.

8.2 1PASSWORD ADMINISTRATION

The Team Lead holds primary admin access. Lee holds secondary admin access. The following steps are required to complete coverage:

- Configure 1Password Emergency Kit and store a physical copy in a secure, institutionally-controlled location (e.g., ERP Manager's office)
- Confirm the ERP Manager has documented knowledge of the emergency access procedure

8.3 CREDENTIAL HYGIENE STANDARDS

- All team credentials are managed exclusively through 1Password — no credentials stored in email, Slack, or personal password managers
- When any team member departs, credentials they had individual access to are rotated
- Access should be scoped appropriately — not all team members require access to all platforms
- Shared credentials are documented with purpose and scope in 1Password notes

09 VENDOR RELATIONSHIPS

Vendor	Purpose	Primary Contact	Contacts Documented
Beacon	Legacy hosting provider	Team Lead	No
WPEngine / 5by5	Incoming hosting provider and support partner	—	In progress

Vendor	Purpose	Primary Contact	Contacts Documented
American Cloud	Server infrastructure for apps.una.edu	No formal contract; support via official support line	Credentials in 1Password; all team members have access

! ACTION REQUIRED
Document the Technical Account Manager (TAM) and Customer Success Manager at Beacon. This information should be accessible to team members and the ERP Manager in the event of Team Lead unavailability.

10 KNOWLEDGE TRANSFER PLAN

PHASE 1 — IMMEDIATE (0–30 DAYS)

- Establish a documented backup process for una.edu database and apps.una.edu WordPress; move backups off Team Lead's local machine
- Document apps.una.edu infrastructure: CloudPanel configuration, American Cloud environment, and SSO/Entra setup
- Document Beacon TAM and customer success manager contacts
- Document response procedure for smallbusinessadvocate.una.edu outages, including third-party contact and escalation path
- Add Tony Bush and Bobby Martin to Claude access
- Record a walkthrough video of critical systems for team reference

PHASE 2 — NEAR-TERM (30–90 DAYS)

- Cross-train at least one developer on WordPress database backup and restoration
- Document all active Banner integration configurations (code is in GitHub; prose documentation does not exist)
- Document all active Slate integration configurations
- Draft runbooks for the five most common support scenarios
- Document response procedure for SSO/Entra failure on apps.una.edu

PHASE 3 — ONGOING

- All new systems must be documented before going into production
- Knowledge transfer is a standing agenda item in team check-ins
- This plan is reviewed and updated quarterly

11 PLAN MAINTENANCE

Activity	Frequency	Owner
Plan review and update	Quarterly	Team Lead
Credential audit	Quarterly	Team Lead
Knowledge transfer session	Bi-annually	Team Lead
ERP Manager review	Annually	Team Lead + ERP Manager

This plan should be treated as a living document. Any significant change to team structure, systems, or platforms triggers an immediate update to the relevant sections.

A DEFINITIONS

- **RTO (Recovery Time Objective)** — The maximum acceptable time to restore a system after failure
- **Runbook** — A documented, step-by-step procedure for a specific operational task
- **Entra** — Microsoft Entra ID, used for SSO across internally developed applications
- **CloudPanel** — Server management panel used to host apps.una.edu on American Cloud infrastructure
- **1Password** — Team credential and secrets management platform
- **Open Alabama** — State reporting platform; the una.edu database is used primarily to support Open Alabama reporting