McLENNAN
COMMUNITY COLLEGE
Information Systems & Services

Multi-Factor Authentication
Implementation Project
Document Version 1.0
Prepared by John Segovia, ISS
Last Edited May 16, 2025

Project Charter

Multi-Factor Authentication Implementation Project

Executive Summary

McLennan Community College (MCC) is committed to protecting its digital infrastructure, institutional data, and the personal information of students, faculty, and staff. As part of this commitment and in alignment with MCC's strategic goals of student success, operational excellence, and caring for people (McLennan Community College, n.d.), the college will implement Multi-Factor Authentication (MFA) using the Duo Security application.

This project aims to enhance identity protection and reduce the risk of unauthorized access to systems by requiring an additional layer of authentication beyond passwords. MFA will be rolled out in a phased approach, starting with the Information Systems and Services (ISS) department followed by faculty, staff, and students.

The project will require collaboration with MCC leadership and departmental stakeholders with a focus on usability, communication, training, and compliance. The estimated project cost is $100K. $72K will be funded by the State and Local Cybersecurity Grant Program through the Office of the Governor of Texas.

Business Need and Background

Eighty-one percent (81%) of web application breaches are traced to stolen credentials (Verizon DBIR 2023). This means that password-only security models are no longer sufficient. Multi-Factor Authentication adds an additional layer during the authentication process that vastly reduces the value of stolen credentials because the bad actor needs an additional factor to gain access.

Identified Needs

Credential Theft Mitigation:

Password compromise continues to be a top attack vector across the education sector. MFA adds a critical second layer of defense to prevent unauthorized access.

Compliance Requirements or Recommendations:

FERPA – mandates the use of "reasonable methods" to protect student education records.

CJIS Security Policy §5.6.2.2 – requires Advanced Authentication (AA) i.e., MFA—for remote access to CJIS data.

NIST 800-171 – Control 3.5.3 mandates MFA for both privileged and remote access to systems handling controlled unclassified information.

HIPAA – requires reasonable and appropriate security measures to protect electronic Protected Health Information (ePHI).

PCI-DSS *v4.0* – Requirement 8.4 mandates MFA for all non-console administrative access and all remote access to the cardholder data environment (CDE).

Secure Remote Access & Bring Your Own Device (BYOD) Support:

With increased remote work, mobile access, and device diversity, MCC needs a solution that can secure both managed and unmanaged devices while balancing barriers to access.

Zero Trust ("never trust, always verify") Strategy Alignment:

Duo's adaptive policies and device trust features support MCC's movement toward zero trust architecture, where access is continually verified based on user, device, location, and context.

Operational Efficiency:

Duo's cloud-based model reduces the need for on-premise infrastructure and minimizes operational overhead through self-enrollment, automatic updates, and administrative dashboards.

Cybersecurity Insurance

Implementing MFA may lower the annual cost of cybersecurity insurance by demonstrating reduced risk and enhanced security controls.

State of Texas

Implementing MFA meets Texas Administrative Code (TAC) 202 controls and increases our compliance with state law.

Strategic Benefits to MCC

Higher education is a top target for credential theft, and compromised accounts can lead to data breaches affecting students, faculty, and staff. Microsoft reports that MFA can block over 99.9% of account compromise attacks, significantly reducing institutional cybersecurity risk (Microsoft 2019).

Manual authentication and logging processes can introduce bottlenecks and inconsistencies across systems such as Learning Management Systems (LMS), Virtual Private Network (VPN), and Human Resource (HR) portals. Duo integrates with authentication systems to automate user authentication, session validation, and access logging—streamlining data flow securely across systems.

Duplicate credential requests or multiple sign-ins lead to confusion, data integrity issues, and greater attack surface. Duo's policy-based authentication streamlines and consolidates login workflows, helping reduce mistyped entries and unauthorized access attempts.

Support staff face heavy demand responding to password resets, account lockouts, and unauthorized access issues. Duo Push allows self-service secure authentication, reducing the need for staff intervention and enabling more efficient operations (Cisco 2022).

Identity theft or unauthorized access to financial aid systems, student grades, or employee records could result in FERPA or HIPAA violations. Duo's contextual and risk-based MFA ensures only verified individuals access sensitive systems defending against stolen credential abuse.

Without insight into login behavior, the college cannot detect suspicious activity or enforce compliance. Duo's dashboard provides real-time analytics and alerting for access attempts, location anomalies, and device health, enabling fast response and policy adjustments.

As MCC expands programs and digital services, we need secure solutions that scale without increasing complexity. Duo is cloud-native and integrates with single sign-on (SSO) providers and hybrid infrastructures, making it scalable for new students, staff, and third-party integrations.

MCC must implement security controls quickly to mitigate current threats without disrupting operations. Duo supports out-of-the-box integrations with popular systems like Microsoft 365, Canvas, and Cisco VPNs, reducing deployment time and training overhead.

Phishing is one of the leading causes of account breaches in education. Even if credentials are phished, MFA prevents access by requiring a second factor the attacker does not have (Verizon DBIR 2023).

The Caring Campus initiative prioritizes student safety, wellbeing, and a culture of trust. MFA protects digital learning environments from disruption and maintains privacy and access integrity, directly supporting the Caring Campus mission.

Project Description and Scope

The project will prioritize the protection of Virtual Private Network (VPN) access and web-based authentication via Single Sign-On (SSO). Duo will be integrated with MCC's existing authentication infrastructure to enforce MFA during logins to core services. As part of a broader transition to an SSO-first architecture, all new services and applications adopted by MCC will be required to use centralized SSO and, by default, be protected by MFA.

In-Scope Services and Deliverables

- Integration of Duo Security with MCC's VPN to require MFA for remote access.
- Enforcement of MFA for Microsoft 365 and other SSO-enabled web applications.
- Deployment of Duo push notifications and passcodes via the Duo Mobile app.
- Centralized device management and monitoring for enrolled users.
- Training materials, user guides, and support documentation.
- Administrative dashboard setup and transfer of service ownership to IT Services.

Out-of-Scope Items

- Google student email accounts (to be addressed in a future phase).
- Physical security controls or campus card access systems.
- MFA for third-party services that do not currently support SSO integration.
- Migration or replacement of non-SSO legacy systems (to be addressed separately).

- Service(s) that are incompatible or not modernized will not be included in this project. However, those services will be migrated later.

This is a new service implementation; no existing MFA service is being retired. However, the project is part of a broader strategic move to SSO as the default authentication method across campus systems. As services are migrated to SSO, they will automatically inherit MFA protection.

Transition Plan Highlights:

- Phase 1: MFA enforced for ISS Employees.
- Phase 2: MFA rolled out to all the MCC community.

Adoption and Scalability Plan:

- Year 1: 100% of the MCC community is required to enroll in Duo MFA for VPN and SSO web access.
- Year 2: Expand to include newly adopted applications.

Duo's cloud-based platform enables seamless scalability with minimal additional infrastructure, making it sustainable for projected adoption rates.

Support Plan and Long-Term Ownership

ISS Cybersecurity Team will own and manage the MFA system for post-deployment.

Support Strategy

- Tier 1 Help Desk support for enrollment, lockouts, and device resets.
- Tier 2 support from the cybersecurity team for policy management and advanced troubleshooting.
- Ongoing training for support staff and documentation updates.

Long-Term Support Strategy

- Hardware: Primary method will be Duo Mobile; hardware tokens will be available on a limited basis, for accessibility compliance, and available for purchase in the McLennan Bookstore (www.mclennanshop.com) for students
- Software: Duo operates via cloud infrastructure, minimizing on-prem maintenance.
- Staffing: Support needs will be re-evaluated annually based on growth and incident volume.

Project Goals

This project has several goals.

Improve Authentication Security for Core Services

- Goal: Implement MFA protection for 100% of VPN access and SSO-based logins by the end of September 2025.
- Success Metric: 85% of full-time employees enrolled in Duo with active devices by deployment deadline; 100% VPN access gated by MFA.
- Threshold: Minimum 75% enrollment within 60 days of Phase 2 launch.

Expand SSO Adoption Across Institutional Services

- Goal: Transition at least three additional high-usage applications to SSO with MFA protection by the end of FY25.
- Success Metric: 100% of selected applications accessible via SSO; 100% access to those systems protected with MFA.
- Transition Metric: Legacy logins disabled for transitioned systems within 15 days of SSO enablement.

Strengthen End-User Awareness and Satisfaction

- Goal: Achieve at least 90% satisfaction from employees on ease of use and perceived security in post-implementation survey (conducted within 30 days of Phase 1 completion).
- Customer Metric: Survey responses showing ≥4.0 average rating on a 5-point scale for usability and support.
- Threshold: No more than 5% of users reporting unresolved enrollment issues during rollout.

Establish a Sustainable Support Model

- Goal: Equip Help Desk with Tier 1 MFA support capabilities and maintain <2 business day resolution time for 95% of MFA-related tickets.
- Technical Metric: First response within 24 hours for all tickets; 100% Help Desk staff trained and certified in Duo admin tasks before full deployment.
- Performance Metric: Monthly incident reports reviewed for patterns in lockouts, failed logins, and user friction.

Project Schedule

Implementation Project Schedule using Duo Security at McLennan Community College (MCC), aligned with MCC's academic calendar (as published at www.mclennan.edu) and structured to minimize disruption to academic operations. This timeline accounts for holidays, end-of-semester transitions, summer downtime, and staff availability.

Key Considerations & Contingencies

- No changes will be made during finals week, graduation, or start-of-term periods (May 5–10 and August 18–29).
- Summer session provides the lowest system usage, ideal for implementation and user support.
- Contingency weeks built into testing and training to allow for staff absences and technical delays.
- Communication plans will be coordinated with campus leadership and public information to ensure awareness before go-live.

PHASE	TIMELINE	FISCAL YEAR	NOTES/ACADEMIC CALENDAR ALIGNMENT
Plan	January – May	2025	Initial planning aligns with Spring semester. Avoids end-of-year system changes. No implementation activities during Spring Break (March 10–14).

PHASE	TIMELINE	FISCAL YEAR	NOTES/ACADEMIC CALENDAR ALIGNMENT
Requirements	Feb	2025	Develop application requirements to provide to vendor for verification.
Solution Analysis	March	2025	Analysis of Duo integration capabilities. Completed prior to Spring Break to ensure continuity. Identify SSO-enabled systems for Phase 1.
Design	May	2025	Occurs after Spring Finals (May 5–10). Includes Duo policy definitions, enrollment workflow design, and support model planning. Request pre-deployment admin accounts.
Code/Build	May – June	2025	Post-semester build window. Integration with VPN. Initial pilot testing (ISS staff only).
Test	June	2025	Conduct system-wide testing. Internal QA. Early user pilot. Adjustments made based on VPN/M365 login behavior and SSO reliability.
Train	July	2025	End-user training for staff/faculty during Summer I and II sessions. Avoids July 4 holiday and ensures Help Desk and Cybersecurity team are fully trained.
Deploy	July	2025	Go-live scheduled for late July, prior to start of Fall 2025 term (August 26). Provides a 3–4-week buffer to stabilize MFA adoption.

Project Budget

The MFA implementation project is a firm-fixed-price engagement based on a one-year subscription model, professional services, hardware, and limited telephony credits. This section provides a breakdown of initial implementation costs and projected post-deployment operations and maintenance (MO&E) costs over a three-year period. It also includes estimates of internal staffing costs (FTE) for support and administration.

Budget Summary – Year 1 Implementation (FY25)

BUDGET ITEM	COST	Details
OOG Grant	$72,000	State of Texas Grant
Hardware/Equipment	$3,270.00	- 150 hardware tokens at $21.80 each
Software, Licensing, and Support	$79,900.00	- $63,000: Duo EDU Advantage – 15,000 students - $16,900: Duo EDU Advantage – 1,300 faculty/staff
Consulting/Implementation	$16,750.00	- Red River Professional Services for deployment, configuration, and training
Telephony Credits	$162.00	15 telephony credit packs (1,000 increments)
Full-Time Employees (FTEs)	$39,150	ISS Employee cost
Total	$139,232	Total deployment cost

Ongoing Maintenance, Operations, and Equipment (MO&E) – FY26–FY28

BUDGET ITEM	FY26	FY27	FY28	Details
Hardware/Equipment	$500	$500	$500	Replacement of ~25 hardware tokens/year

Software, Licensing, and Support	$79,900	$79,900	$79,900	Annual Duo Advantage license renewal (based on Year 1 quote, subject to inflation)
Telephony Credits	$162	$162	$162	Optional usage based on needs
Total	$80,562	$80,562	$80,562	-Total per FY

Project Management and Governance

ROLE	NAME	ORGANIZATION
Executive Sponsor	Johnette McKown	President
Executive Sponsor	Chadwick Eggleston	Vice President of Instruction & Student Engagement
Executive Sponsor	Mark Harmsen	Vice President of Finance & Administration
Executive Sponsor	Laura Wichman	Vice President of Strategic Planning and Enrollment
Project Oversight	Mario Leal	Chief Information and Technology Officer
Project Team (Manager)	John Segovia	Cybersecurity and Online Technology Manager
Project Team (Technical Lead)	H. Nielsen	Cybersecurity Application and Support Specialist
Project Team	Daniel Brown	Cybersecurity Application and Support Specialist
Project Team	Laura J. Crapps	Cybersecurity Business Analyst
Infrastructure Point of Contact	Noah Daly	Infrastructure Manager
Customer Support Services Point of Contact	David Kuehne	Customer Support Services Manager
Administrative Systems Point of Contact	Vickie Peterson	Administrative Systems Manager

Impact Analysis

The implementation of Duo Security for Multi-Factor Authentication (MFA) will impact multiple stakeholders, business areas, and technical systems across MCC. These impacts are primarily associated with the enhanced security requirements for system access and the operational adjustments required to support MFA and Single Sign-On (SSO) integrations.

Impacted Community Members

- Faculty & Staff
    - Required to enroll in Duo MFA to access VPN, Microsoft 365, and SSO-protected systems. May need to install Duo Mobile or use hardware tokens.
- ISS Services
    - Responsible for configuring, supporting, and maintaining the MFA infrastructure. Helpdesk will handle first-tier support for enrollments and issues.
- Cybersecurity Team
    - Gains improved visibility and control over access events. Responsible for policy enforcement, reporting, and threat response.

Impacted Teams

- Information System Services
    - Major responsibility for Duo integration, SSO migration, and long-term system monitoring.
- Academic Services

  - Faculty and instructional staff must authenticate via Duo for access to systems like Brightspace and Zoom.
- Human Resources
  - Coordination with IT for onboarding/offboarding processes with MFA enrollment and SSO provisioning.

Impacted Systems

- VPN (GlobalProtect)
  - MFA will be required for remote network access, affecting all remote faculty and staff.
- Microsoft 365 / Entra AD
  - MFA will be enforced at login for cloud email, Teams, and productivity tools.
- SSO Platform (SAML)
  - SSO-enabled systems (e.g., Brightspace, Softdocs, Zoom) will be protected by MFA upon transition.
- Helpdesk Tools
  - SOPs will be updated to reflect MFA support procedures including enrollment assistance and token replacement.

Assumptions

These assumptions are based on current conditions, stakeholder input, and industry's best practices.

Technical Assumptions

1. MCC's existing identity provider is stable and can support Duo SSO integrations.

2. VPN client currently deployed is compatible with Duo's authentication proxy.

3. Network configurations, firewall rules, and internal systems will allow traffic required for Duo's cloud services.

4. Recent infrastructure changes (e.g., domain migration, identity management) are actively in use and stable.

User and Operational Assumptions

6. Faculty, staff, and student users will comply with enrollment deadlines and complete MFA setup with minimal resistance.

7. Help Desk staff will complete Duo training prior to general deployment and can manage first-tier support requests.

8. Sufficient documentation and communications will be prepared to support user onboarding and self-service troubleshooting.

Vendor and Implementation Assumptions

10. The vendor will deliver services in accordance with the Statement of Work (SOW), including project kickoff, configuration, testing, and knowledge transfer.

11. All licensing, hardware tokens, and support services will be delivered on time and without procurement or shipping delays.

12. MCC's cybersecurity project team will provide timely responses to the vendor and make internal resources (cybersecurity and infrastructure staff) available as scheduled.

Budget and Resource Assumptions

13. Funding for initial implementation and three years of maintenance and support is approved and will remain stable.

14. Staff time allocated for implementation (e.g., projected FTE time allotments for cybersecurity and support roles) will be maintained throughout the rollout period.

Constraints

This project has several constraints.

Time Constraints

1. Grant funding for the MFA project must be fully utilized prior to August 30, 2025.

    - All procurement (hardware, licensing, services) and invoicing must be completed before this date.

    - Delays beyond this deadline risk forfeiting unspent funds or noncompliance with funding guidelines.

2. The deployment must avoid academic disruption during key periods:

    - Spring finals (May 5–10, 2025)

    - Fall semester start-up (August 18–29, 2025)

    - Holidays and summer break periods must be considered in scheduling training and testing.

    - Summer Hours - 36 hours per week, with half the Cybersecurity team working M-Th. and the other half Tue.-Fri.

Resource Constraints

3. Internal staffing is limited to 36-hour work weeks per "Summer Hours" for cybersecurity support throughout the project. The availability of technical staff outside of business hours is constrained.

4. Help Desk and training resources are shared across other ISS initiatives and may not be exclusively available for MFA support.

Technical Constraints

5. MFA coverage is currently limited to systems integrated with the existing identity provider. Legacy applications without SSO capabilities are out of scope until further modernization.

6. Duo hardware tokens are limited in quantity (150 initially). Users without smartphones or staff who do not want to deploy the app on a personal device.

Vendor and Support Constraints

7. Red River Technology's implementation timeline requires a minimum two-week notice post-purchase order before beginning work.

8. All professional services are based on standard business hours (8am–5pm CST, M–F); off-hours support requires special coordination and may incur additional costs.

Risks

The MFA implementation project at McLennan Community College faces several critical risks that must be actively monitored and mitigated.

- The most immediate and high-priority risk is the requirement to fully expend all grant funding by August 30, 2025. Failure to do so could result in the loss of funds and noncompliance with grant conditions. To mitigate this, all licensing, hardware, and service procurements will be completed and invoiced by May 31, 2025, with weekly tracking of expenses by the project team.
- Another moderate-to-high risk involves potential delays in the service delivery timeline by the implementation partner. Given the compressed summer schedule and the need to avoid disruption at the start of the fall semester, such delays could jeopardize the rollout timeline. This risk will be mitigated by early milestone planning, pre-scheduling configuration windows, and maintaining constant communication with the vendor's project manager.
- There is also a moderate risk of low enrollment or resistance from faculty and staff, particularly among users unfamiliar with MFA. If adoption is slow, this could place additional strain on ISS resources and compromise the security posture. MCC will address this through targeted awareness campaigns, training materials, and clear mandates that enforce MFA enrollment before the fall semester begins.
- The Help Desk's capacity to support the rollout presents another moderate risk. With limited FTE availability, especially during peak times, delays in resolving MFA issues may lead to user dissatisfaction. This risk will be addressed by staggering deployments by department, extending support staff during go-live, and using self-service tools and SOPs.
- From a technical perspective, incompatibility with legacy systems that lack SSO support poses a high risk to full coverage. Some systems may not be able to integrate with Duo MFA until modernized. MCC will catalog these systems, prioritize them for future phases, and develop policy exceptions to maintain overall security posture in the interim.

- There is a low risk related to hardware token availability, as only 150 tokens are included in the initial procurement. While most users are expected to enroll using the Duo Mobile app, some may require alternative options. MCC will explore additional token orders if demand exceeds projections.

Bibliography

Cisco. (2021). *Duo Security: Product Overview*. https://duo.com/resources.

Cisco. (2022). *Duo Push: User Experience and Help Desk Impact*. https://duo.com/blog

Federal Bureau of Investigation. (2022, June 1). *Criminal Justice Information Services (CJIS) Security Policy Version 5.9*. U.S. Department of Justice. https://www.fbi.gov/file-repository/cjis-security-policy-version-5-9-20220601.pdf/view

Health and Human Services. (2022). *Multi-factor authentication FAQs*. U.S. Department of Health and Human Services. https://www.hhs.gov/sites/default/files/mfa-faqs.pdf

National Institute of Standards and Technology. (2020). *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (NIST SP 800-171 Rev. 2)*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

McLennan Community College. (n.d.). Strategic plan 2020–2025. https://www.mclennan.edu/strategic-planning/

Microsoft. (2019). *Your Pa$$word doesn't matter*. https://www.microsoft.com/security/blog/2019/01/15/your-password-doesnt-matter

Payment Card Industry Security Standards Council. (2022). *Payment Card Industry Data Security Standard: Requirements and Testing Procedures, Version 4.0*. https://docs.prismacloud.io/en/enterprise-edition/policy-reference/compliance-policies/pci-dss-v4-0

U.S. Department of Education, Privacy Technical Assistance Center. (2015). *Data Security: FERPA and best practices for electronic student records*. https://studentprivacy.ed.gov/resources/ferpa-and-information-security-best-practices

Verizon. (2023). *Data Breach Investigations Report (DBIR)*. https://www.verizon.com/business/resources/reports/dbir/

Revision History

Version	Date	Updater Name	Description
V 0.1	3/28/2025	Mario Leal	I took John Segovia's initial ideas and put them into this template. Then, I edited and provided tips for filling out the rest of the sections.
V 0.2	3/31/2025	John Segovia	I have begun making corrections and have asked ML to finish identifying section responsibilities.
V 0.3	4/22/2025	John Segovia	Fleshed out benefits and needs.
V 0.4	5/7/2025	John Segovia	Final draft submitted to CITO for review.
V 0.5	5/13/2025	Mario Leal	Review, added comments, and made some recommendations for deletions and edits.
V 1.0	5/13/2025	John Segovia	Document ready for release.