

TECH & AI CASE STUDY - UNIVERSITY - 2026

SSO and MFA for 30,000 Users That Cut Helpdesk Tickets 52%

Based on a delivery engagement with Kestrel Valley University

-52%

PASSWORD-RESET TICKETS

98%

MFA ADOPTION

**40 to 2 per
semester**

ACCOUNT-TAKEOVER INCIDENTS

63

FEDERATED APPLICATIONS

A fillable practice edition: the full story, 8 actions,
6 reflections and a 90-day plan - work it with your team.

Free - no email required
emersontechnology.com

MAKE THIS PRACTICE BOOK YOURS

Work it, do not just read it

This practice book turns the Kestrel Valley University case study into a working session for your team. Read the full story first - what happened, what was built and what it changed. Then tick the 8 actions you can commit to, write short answers to the 6 reflections, and finish with a 90-day plan. Every field in this PDF is fillable: open it in Adobe Acrobat Reader, Chrome, Edge or macOS Preview, type directly into the boxes and save.

YOUR NAME	ROLE
COMPANY	TEAM / DEPARTMENT
DATE	EMAIL (OPTIONAL)

MY GOAL FOR THIS PRACTICE SESSION

- 01 The story** - What happened at Kestrel Valley University - before, during and after the project.
- 02 The results** - The numbers that changed, plus industry benchmarks from public research.
- 03 The 8-action checklist** - Tick boxes as your organization completes each step. Owner and date fields included.
- 04 The 6 reflections** - Fillable questions that pressure-test your own roadmap.
- 05 My 90-day plan** - Three fillable phase cards that turn this case study into your roadmap.

RUN IT AS A 90-MINUTE TEAM SESSION

25 min READ Read the story together. Ask everyone to note the one number that surprised them most.	40 min PRACTICE Work the 8-action checklist and the 6 reflections. Assign an owner and a date to every action you commit to.	25 min COMMIT Fill in the 90-day plan. One goal per phase, one number that tells you it worked. Book a review date before you leave the room.
--	--	---

THE STORY

What happened, and why it worked

01 The Company

Kestrel Valley University is a comprehensive public institution serving 30,000 students and 3,400 employees across undergraduate, graduate and continuing-education programs. Its technology estate reflects a university's characteristic history: a student information system older than most of its users, learning platforms adopted college by college, finance and HR systems serving the administration, and a long tail of departmental applications accumulated over decades. Identity touches every one of those systems, several times over, for every person who studies or works there.

The university's IT organization was competent but stretched, operating with the seasonal rhythm that defines academic computing: everything is quiet during breaks and everything is urgent during registration. The service desk in particular lived a boom-and-bust cycle, absorbing thousands of routine requests each term while simultaneously supporting research computing and classroom technology. The CIO's standing constraint was political as much as technical — any identity change that disrupted registration week, delayed payroll or interrupted a research workflow would consume more goodwill than the project could survive. The program therefore had to succeed quietly, inside the gaps the academic calendar left open.

02 Where Things Stood

Before the program, an average student needed 14 separate application logins, and the university's systems for managing them had eroded into a combination of exports and hope. The service desk logged roughly 6,800 password-reset tickets a year, each one a manual identity verification and reset performed by an agent. Deprovisioning depended on manual lists: when a student withdrew or an employee departed, someone compiled a spreadsheet of affected systems and worked through it, so departing students routinely retained access to licensed software for months after they were gone. Nobody regarded this as acceptable; everybody regarded it as normal.

Security pressure was mounting on the same infrastructure. Phishing campaigns targeting student-finance credentials — emails impersonating the bursar's office, financial aid and work-study payroll — grew more convincing each semester, and the fall term closed with more than 40 confirmed account takeovers. A compromised student finance account meant redirected disbursements and weeks of remediation for the affected student; a compromised staff account meant something worse. Dozens of shared departmental passwords circulated for lab equipment, display systems and legacy tools, none of them tied to an individual and none of them revocable.

Auditors made identity management the university's highest-rated risk, and the finding carried weight because it was impossible to argue with: the university could not demonstrate who had access to what, nor prove that access ended when someone left. The CIO needed a fix that satisfied auditors, cut the ticket load and improved the student experience, all without stalling registration or research. Microsoft security research reportedly finds that multi-factor authentication blocks over 99.2% of account compromise attacks — the largest single control improvement available to most organizations — which made MFA the anchor, but the challenge was delivering it to 30,000 people who had not asked for it.

03 The Challenge

The challenge decomposed into three problems that had to be solved in a specific order. First, fragmentation: with 14 logins per student and dozens of departmentally held passwords, every security control had to be repeated 14 times and every user experience was 14 times worse than it needed to be. Second, lifecycle: as long as access was granted and revoked through emailed spreadsheets and manual lists, no audit finding would ever close, because the evidence trail did not exist. Third, adoption: MFA imposed on an unwilling population of 30,000 students could produce a revolt or a helpdesk meltdown, and either would set the program back a year. The Verizon Data Breach Investigations Report has repeatedly identified stolen credentials as a leading initial access vector, with education among the most-targeted sectors, so the risk side of the ledger was unambiguous. The constraint side was equally real: enrollment waves could not collide with registration, employee rollouts could not collide with semester start, and the service desk could not absorb a spike of confused users on top of its existing 6,800 tickets. NIST's digital identity guidelines, SP 800-63B, advise screening passwords against breach corpora and dropping forced periodic rotation — guidance the university adopted — but the deeper work was architectural: one identity provider, one lifecycle engine, and an enrollment experience designed around the moments when students and staff are already changing settings.

04 Discovery and Diagnosis

Emerson Technology began with a four-week discovery across the application estate, the service desk's ticket history and the identity data sources. Ticket analysis ranked every application by the password-reset burden it generated, producing an objective federation order: the five noisiest systems accounted for a disproportionate share of the 6,800 annual tickets, so federating them first would fund the rest of the program in visible savings. The application census catalogued all systems in use, their authentication methods and their owners, and it surfaced 47 shared departmental accounts whose purposes ranged from legitimate automation to pure habit. Diagnosis interviews with the service desk, the registrar and department administrators mapped the academic calendar's hard constraints and the human workflows around them. The student information system and the HR platform emerged as the authoritative sources of truth for who should have access — which meant SCIM provisioning wired to those two systems could replace the manual lists entirely. The diagnosis also flagged a cultural fact the rollout plan had to respect: students configure their lives during orientation, employees during onboarding, and neither population responds to email campaigns sent at random moments. The final discovery output was a sequenced, calendar-aware rollout plan with named phases, support staffing plans and a public metrics commitment.

05 The Solution

The program consolidated identity into a single cloud identity provider and rebuilt the university's access model around it, delivered in waves that respected the academic calendar.

One provider, federated in ticket order

Sixty-three applications were federated through SAML and OIDC onto the new identity provider, sequenced by ticket volume so the five systems generating the most password resets went first and the savings appeared immediately. Group-based entitlements replaced the per-app access spreadsheets, giving every application a defined set of groups with named owners instead of undocumented grant lists. Self-service password reset with verified recovery was deployed before enforcement began, because it removes the single largest ticket category at its source and softens the overall experience for users encountering the new system. Within a semester, the service desk's queue had transformed from a password-reset factory into a genuine support function.

MFA in waves, timed to the calendar

MFA rolled out in enrollment waves by role. Employees went first, with FIDO2 hardware keys issued to finance and administration staff whose accounts could move real money; students followed through an authenticator-app rollout with recovery-code ceremonies built directly into orientation, so enrollment happened where students already expected to configure their accounts rather than through email campaigns. The helpdesk was prepared for wave one — trained on recovery scenarios, staffed with extra hours for peak weeks — because the helpdesk experience decides whether MFA feels helpful or hostile. Meeting users inside orientation and onboarding flows roughly doubled enrollment completion rates compared with the pilot email push, and the waves kept support load predictable through the term.

Lifecycle automation and the shared-account cleanup

SCIM provisioning connected the student information system and HR platform to the identity provider, so access now grants and revokes automatically within hours of enrollment changes — a student who withdraws mid-term loses licensed software access the same day, and the audit evidence trail exists by construction. Legacy shared accounts were retired through a documented exception process: each account received a named owner, a documented purpose and an expiry date, and accounts that could not justify themselves were decommissioned. Exceptions that can be seen and scheduled die quietly; invisible ones persist for years. Password guidance was also modernized to align with NIST SP 800-63B — breach-corpus screening instead of forced periodic rotation — which reduced user friction while raising actual security.

06 The First 90 Days

The program's first quarter was timed to land between terms. Weeks one through four covered discovery, the application census and the identity provider deployment in audit-only mode. Weeks five through eight federated the first five ticket-generating applications and launched self-service password reset, and the effect on the service desk was immediate: reset volume began dropping even before MFA enforcement, as users recovered their own credentials through verified flows. The service desk used the breathing room to train for the MFA waves, building a recovery playbook and staffing plan for the enrollment surge.

Weeks nine through twelve delivered the employee MFA wave and the first student wave, both scheduled against the calendar the diagnosis had mapped. Hardware keys were issued to finance and administration with in-person enrollment sessions; students enrolled during orientation with recovery-code ceremonies, and the helpdesk's expanded hours absorbed the question volume without overtime. The shared-account amnesty ran concurrently: departments claimed or retired their 47 accounts, each claim requiring a named owner and expiry date. By day 90, offboarding completed within hours for new departures, the first registration week under the new model passed without a helpdesk spike, and leadership received the program's first public metrics report — adoption, ticket volume and takeover counts — establishing the cadence that would carry the program through the full 63-application federation.

07 The Results

Password-reset tickets fell 52% — from 6,800 to roughly 3,260 a year — freeing the service desk for higher-value work across the institution. MFA adoption reached 98% of active accounts, and confirmed account takeovers dropped from more than 40 per semester to two. Offboarding now completes within hours, closing the auditor's top finding a full year ahead of schedule, and registration-week load no longer spikes the helpdesk because most resets are self-service rather than agent-assisted.

METRIC	BEFORE	AFTER
Password-reset tickets	-	-52%

METRIC	BEFORE	AFTER
MFA adoption	-	98%
Account-takeover incidents	40	2 per semester
Federated applications	-	63

The second-order effects have proven durable. Auditors moved identity from highest-rated risk to a control the university can demonstrate with system-generated evidence, and the service desk reports that its registration-week staffing now goes to genuine enrollment questions rather than password resets. Departments that once shared passwords now manage group memberships, and the group-based entitlement model gives system owners a way to see — and answer for — who can reach their applications. The two residual account takeovers per semester are investigated with full session and MFA telemetry rather than guesswork, which is the difference between an incident and a mystery.

08 What Your Business Should Do

The university's playbook transfers to any large organization drowning in fragmented logins and manual lifecycle work. Consolidate identity into one provider and federate applications through SAML or OIDC in ticket-volume order — starting with the noisiest systems funds the rest of the program in visible savings. Roll MFA out in waves by role, enrolling high-risk roles first with phishing-resistant hardware keys, then general users and students in scheduled waves, because staggered rollout prevents registration-week chaos and keeps support load predictable. Connect provisioning to your authoritative source systems with SCIM or an equivalent, so access grants and revokes automatically instead of through emailed spreadsheets and manual lists. Deploy verified self-service password reset before MFA enforcement begins; it removes the single largest ticket category and softens the enrollment experience at the same time.

Retire shared accounts through a visible exception process — every account gets a named owner, a documented purpose and an expiry date, because exceptions you can see and schedule die quietly while invisible ones persist for years. Time enrollment around the moments users already change settings, building MFA into orientation, onboarding and registration flows rather than email campaigns; meeting users where they are roughly doubles completion rates. Prepare the helpdesk for wave one with trained recovery scenarios and extra staffing for peak weeks, since the helpdesk experience decides whether MFA feels helpful or hostile. Finally, track adoption and tickets publicly — publish MFA adoption, reset volume and takeover counts to leadership monthly, because visible numbers keep enrollment waves scheduled and justify the next phase of identity work. Work this eight-step sequence into your next academic term with the action checklist in this practice book, and bring the reflection questions back each semester: how many logins does an average user need, how long does it take to revoke access for someone who leaves mid-term, and would your auditors rank identity management as your highest risk too?

REAL-WORLD PROOF & BENCHMARKS

Microsoft security research reportedly finds multi-factor authentication blocks over 99.2% of account compromise attacks, the largest single control improvement available to most organizations. - Microsoft security research

The Verizon Data Breach Investigations Report has repeatedly identified stolen credentials as a leading initial access vector, with education among the most-targeted sectors. - Verizon DBIR, 2024

NIST's digital identity guidelines, SP 800-63B, advise screening passwords against breach corpora and dropping forced periodic rotation — guidance many institutions still lag on. - NIST SP 800-63B

THE PRACTICE PAGES

The 8-action checklist

Work through the list with your team. Tick each box as your organization completes the step, and fill in an owner and a target date so every action has a name and a deadline.

☐

1. Consolidate identity into one provider

Pick a single identity provider and federate applications through SAML or OIDC in ticket-volume order. Starting with the noisiest systems funds the rest of the program.

OWNER

TARGET DATE

STATUS

--	--	--

☐

2. Roll MFA out in waves by role

Enroll high-risk roles first with phishing-resistant hardware keys, then general users and students in scheduled waves. Staggered rollout prevents registration-week chaos and keeps support load predictable.

OWNER

TARGET DATE

STATUS

--	--	--

☐

3. Connect provisioning to source systems

Wire SCIM or equivalent automated provisioning to your student information system and HR platform. Access should grant and revoke automatically, never through emailed spreadsheets and manual lists.

OWNER

TARGET DATE

STATUS

--	--	--

☐

4. Offer self-service password reset

Deploy verified self-service password reset with secure recovery codes before MFA enforcement begins. It removes the single largest ticket category and softens the overall enrollment experience for users.

OWNER

TARGET DATE

STATUS

--	--	--

☐

5. Retire shared accounts with exceptions

Move every shared account to named owners, documented purpose and an expiry date. Exceptions you can see and schedule die quietly; invisible ones persist for years.

OWNER

TARGET DATE

STATUS

--	--	--



6. Time enrollment around the calendar

Build MFA enrollment into orientation, onboarding and registration flows rather than email campaigns. Meeting users where they already change settings roughly doubles completion rates and reduces support load.

OWNER

TARGET DATE

STATUS

--	--	--



7. Prepare the helpdesk for wave one

Train service-desk staff on recovery scenarios before the first enrollment wave, and staff extra hours for peak weeks. The helpdesk experience decides whether MFA feels helpful or hostile.

OWNER

TARGET DATE

STATUS

--	--	--



8. Track adoption and tickets publicly

Publish MFA adoption, reset volume and takeover counts to leadership monthly. Visible numbers keep enrollment waves scheduled and justify the next phase of identity work.

OWNER

TARGET DATE

STATUS

--	--	--

AFTER THE CHECKLIST: OUR TOP 3 PRIORITIES

From the eight actions above, write down the three you will start first - and the single number you expect each one to move. Three priorities with owners beat eight without any.

PRIORITY 1 NUMBER IT SHOULD MOVE	PRIORITY 2 NUMBER IT SHOULD MOVE	PRIORITY 3 NUMBER IT SHOULD MOVE
--	--	--

THE PRACTICE PAGES

Reflections for your team

Use these questions in your next planning session and type short answers into the boxes. The gaps you find are usually the fastest wins.

Q1. How many separate logins does an average student need at your institution — and who actually knows the answer?

Q2. What would your helpdesk do with the hours currently spent resetting passwords every semester?

Q3. How long does it take today to revoke access for a student who withdraws mid-term?

Q4. Which departments still share accounts, and does anyone know what those accounts can actually reach?

Q5. If phishing doubled next semester, how many finance or research accounts would you expect to lose?

Q6. Would your auditors rank identity management as your highest risk too — and what evidence would change their minds?

THE PRACTICE PAGES

My 90-day plan

Finish the session by committing to a plan. Three phases, one goal each, one number that tells you it worked. Bring this page to your next leadership review - or to a free consultation with Emerson Technology, and we will pressure-test it with you.

Days 1-30 Focus: audit and alignment

PRIMARY GOAL**KEY ACTIONS****HOW WE MEASURE SUCCESS****OWNER**

Days 31-60 Focus: build and prove

PRIMARY GOAL**KEY ACTIONS****HOW WE MEASURE SUCCESS****OWNER**

Days 61-90 Focus: scale and measure

PRIMARY GOAL

KEY ACTIONS

HOW WE MEASURE SUCCESS

OWNER

Tip: save a copy per team so each group keeps its own answers. Revisit the reflections every quarter - the questions stay the same even as the numbers move.

BOOK THE REVIEW BEFORE YOU CLOSE THE BOOK

Plans without a review date drift. Before you close this practice book, agree on when you will come back to these pages, who will run that session, and when you will check the numbers again. If you want an outside pair of eyes, bring this page to a free consultation with Emerson Technology and we will pressure-test the plan with you.

REVIEW DATE	REVIEWED BY	NEXT CHECK-IN

Ready for a transformation like Kestrel Valley University's?

Emerson Technology designs and builds the data, AI, cloud and automation systems behind results like these. On a free consultation call we will map this exact playbook to your business - your data, your constraints, your numbers.

Book a free consultation

support@emersontechnology.com

or start online: emersontechnology.com/contact