

Phase 2 Project Scope

RapidIdentity Platform Expansion

Prepared for: DeKalb County School District

1. Scope Summary

Following a successful Phase 1 implementation of RapidIdentity, **DeKalb County School District** would like to expand the platform through a series of additional services. Phase 2 is organized around four primary initiatives:

- Transition the Staff Source of Authority (SoA) from EnumDB to MUNIS, with account lifecycle for all remaining user types covered by dedicated RapidIdentity Workflows.
- Integration with Incident IQ, **DeKalb County School District's** IT ticketing platform, to serve as the form and request origin for select user-type workflows.
- Frontline → RapidIdentity → Canvas provisioning pipeline, enabling pre-hire Canvas access via Frontline applicant data and automated staff provisioning from MUNIS to Canvas.

Workflows for user types that fall outside of the MUNIS HR feed will leverage the RapidIdentity Sponsorship Module where applicable, with sensitive data stored in a secure database. Workflows currently managed via email and spreadsheet will be formalized and automated within RapidIdentity.

2. Scope of Work

2.1 MUNIS as Staff Source of Authority

The existing EnumDB database will be retired as the primary staff SoA. The RapidIdentity Staff Import job will be reconfigured to consume staff records directly from the MUNIS HR database. For user types that are not present in the MUNIS HR data feed, dedicated workflows (described in Section 2.3) will govern account lifecycle, using the RapidIdentity Sponsorship Module where appropriate.

Key activities include:

- Assessment and documentation of current EnumDB data structure and field mappings.
- Reconfiguration and testing of the RapidIdentity Staff Import job to use MUNIS as the authoritative data source.
- Validation of attribute mapping between MUNIS and RapidIdentity.
- Parallel-run testing to confirm parity before EnumDB is decommissioned.

- Definition of a formal cutover and EnumDB decommission plan.

2.2 Incident IQ Integration

RapidIdentity will be integrated with Incident IQ for the applicable workflows listed in Section 2.3. During the design phase, both parties will evaluate and agree upon an integration pattern:

- Inbound API (Incident IQ → RapidIdentity): Upon ticket submission in Incident IQ, an API call triggers the corresponding RapidIdentity workflow.
- Outbound Polling (RapidIdentity → Incident IQ): RapidIdentity periodically queries the Incident IQ API to identify new requests and processes them.

Additionally, the design phase will include an evaluation of whether Incident IQ or RapidIdentity's native form capability is the preferred request submission interface for each applicable workflow. RapidIdentity's built-in forms may fully replace Incident IQ as the form layer depending on **DeKalb County School District's** preferences.

Where configured, workflows will include an approval step — routing requests to the requestor's manager or a designated approver group before provisioning is executed.

2.3 Account Lifecycle Workflows

RapidIdentity Workflows will be designed, built, and tested for the user types listed below. Workflows are grouped by integration method. Each workflow covers the full account lifecycle (creation, modification, deactivation).

Workflows Using Incident IQ

The following user types will use Incident IQ (or RapidIdentity native forms, to be determined during design) as the request intake mechanism:

- College Teachers / Schools (Post-Secondaries)
- Substitutes – Short Term & Long Term
- In-State & Out-of-State Transfer Teachers
- IC Scheduling N-Numbers (Additional Employee Accounts for Scheduling)

Workflows Not Using Incident IQ

The following user types will be provisioned via internal RapidIdentity workflows without an Incident IQ intake step. Where noted, the Sponsorship Module will be leveraged and sensitive data will be stored in a secure database.

- Contractor Teacher / Staff for IC Enterprise – C-Number Sponsorship — Sponsorship module; sensitive data stored in secure DB

- Lead Teacher SPED, Speech Language Pathology, Occupational Therapy (E9800s) — currently managed via email and tracked in a spreadsheet; to be formalized in RapidIdentity
- Itinerant Teachers — secondary MUNIS data sourced from the HR staff file table
- Interim Principals, Assistant Principals, Counselors — MUNIS data sourced from the HR staff file table
- Gnet Teachers — MUNIS data sourced from the HR staff file table

During the design phase, each workflow will be evaluated to determine the most appropriate implementation approach. The design will determine whether each workflow is best delivered as:

- A RapidIdentity Workflow through the Requests Module, or
- Manual entry using the RapidIdentity People Module Delegations.

2.5 Frontline → RapidIdentity → Canvas Provisioning

RapidIdentity will serve as the central provisioning hub connecting Frontline, MUNIS, and Canvas. This pipeline enables two provisioning flows: (1) Frontline Import — applicant records are sourced from Frontline via API (preferred) or CSV export and provisioned into RapidIdentity, then into Canvas, enabling pre-hires to complete onboarding paperwork before their official hire date. A unique Frontline identifier is stored on the pre-hire account so that when the individual is hired into MUNIS, RapidIdentity updates the existing account with no duplicates created. (2) Canvas Export — regular staff sourced from MUNIS are automatically provisioned into Canvas via RapidIdentity, replacing the current manual account creation process. Canvas API access and Frontline data availability must be confirmed during the design phase before build begins.

2.6 Required Customer Resources

Successful delivery of this engagement requires active participation from **DeKalb County School District** personnel with administrative access and decision-making authority for each in-scope system. The following System Administrators and Stakeholders must be identified and made available throughout the project:

- **MUNIS** – System Administrator and HR/Payroll Stakeholder with access to HR data feeds and ability to confirm field mappings.
- **Infinite Campus** – System Administrator with access to SIS configuration, scheduling data, and N-Number/C-Number account structures.
- **Frontline** – System Administrator and Stakeholder able to confirm API access, applicant data exports, and unique identifier configuration for pre-hire records.
- **Canvas** – System Administrator with API access and ability to confirm provisioning requirements for staff and pre-hire accounts.
- **Incident IQ** – System Administrator with API access and ability to configure ticket forms, workflow triggers, and integration settings.

3. Project Phases

This engagement is delivered across five structured phases. Each phase has defined objectives and entry/exit criteria to ensure quality and alignment before proceeding.

3.1 Readiness

Ensuring all necessary access to source and target systems is in place before design begins. This includes confirming credentials, API tokens, sandbox environments, and stakeholder availability.

Estimated duration: less than 1 week

3.2 Design

Creation and collaborative review of a Solution Design Document (SDD) that provides a high-level overview of what will be built, including data flows, workflow logic, integration patterns, and system configurations. The SDD requires customer review, approval, and signature before the project proceeds to the Build phase.

Estimated duration: 2–6 weeks

3.3 Build

Implementation of the approved solution design. Identity Automation engineers configure RapidIdentity workflows, integrations, and provisioning rules per the signed SDD. Unit testing is conducted throughout.

Estimated duration: 2–4 weeks

3.4 User Acceptance Testing

Customer testing of the built solution using pre-determined test cases provided by Identity Automation. Test users and groups must be available prior to this phase. Successful completion of all test cases constitutes readiness for launch.

Estimated duration: 1–2 weeks

3.5 Solution Launch

Activation of the new solution in production and formal retirement of any legacy manual processes or workflows being replaced. Knowledge transfer is completed and the customer assumes ownership of the running solution.

4. Success and Acceptance Criteria

4.1 MUNIS Source of Authority Migration

- RapidIdentity Staff Import job successfully reads and processes staff records from MUNIS.
- All required staff attributes are accurately mapped with no data loss or corruption.

- EnumDB is no longer required as a data source for any RapidIdentity provisioning process.
- Parallel testing confirms provisioning outcomes are equivalent to or better than the previous EnumDB-based process.

4.2 Incident IQ Integration

- Agreed-upon integration pattern is implemented and verified end-to-end for all applicable workflows.
- Requests submitted via the designated form trigger the correct RapidIdentity workflow.
- Approval routing (where configured) correctly routes to the designated approver and only proceeds upon approval.

4.3 Account Lifecycle Workflows

- All nine (9) Account Lifecycle Workflows are built, tested, and deployed to production.
- Sponsorship workflows correctly leverage the Sponsorship Module and store sensitive data in the designated secure database.
- Workflows previously managed via email/spreadsheet (E9800s) are fully replaced by automated RapidIdentity processes.
- Each workflow correctly provisions, modifies, or deprovisions accounts per documented design specifications.
- **DeKalb County School District** confirms successful end-to-end testing of each workflow prior to sign-off.

4.4 Canvas Provisioning

- Pre-hire applicants from Frontline are provisioned into RapidIdentity and Canvas prior to their official hire date, confirmed by successful end-to-end testing. When a pre-hire is hired into MUNIS, their existing account is updated with no duplicate accounts created. Regular staff from MUNIS are automatically provisioned into Canvas, eliminating the current manual account creation process. **DeKalb County School District** confirms successful testing of both provisioning flows prior to sign-off.

4.5 General

- All deliverables reviewed and accepted by **DeKalb County School District's** designated project stakeholder(s).
- Knowledge transfer completed for all implemented components.
- No critical or high-severity defects remain open at project closure.

5. Risks

The following risks have been identified. Each will be revisited and refined during project kick-off and the design phase.

Risk	Likelihood	Impact	Mitigation
MUNIS API or data structure does not align with expected staff record schema	Medium	High	Conduct data-mapping workshop during design phase to validate all fields before development begins.
Incident IQ API constraints limit integration options for applicable workflows	Medium	Medium	Evaluate API documentation and sandbox access early; RapidIdentity native forms available as fallback.
Manual workflows (email/spreadsheet-based) lack sufficient documentation to automate accurately	Medium	Medium	Facilitate a requirements workshop with process owners before design begins to capture all current-state logic.
Frontline → RapidIdentity → Canvas: Frontline API or data availability constraints could delay integration	Medium	Medium	Confirm Canvas API access and Frontline API/export availability during design phase. Validate unique identifier field for pre-hire-to-hire account matching. Identify CSV-based fallback if Frontline API is unavailable.
Customer approval/decision delays extend project timeline	Medium	Medium	Establish named stakeholders and decision timelines at kick-off. Build review windows into the project schedule.

6. Hours Breakdown

The following table summarizes estimated professional services hours for all in-scope deliverables. Each Account Lifecycle Workflow is allocated 16 hours. The Frontline → RapidIdentity → Canvas provisioning is split into two line items: Frontline Import Provisioning (24 hrs) and Canvas Export Provisioning (24 hrs).

Deliverable / Workflow	User Type / Description	Integration	Hours
WORKFLOWS – via IncidentIQ			
Account Lifecycle Workflow	College Teachers / Schools (Post-Secondaries)	Incident IQ	16
Account Lifecycle Workflow	Substitutes – Short Term & Long Term	Incident IQ	16
Account Lifecycle Workflow	In-State & Out-of-State Transfer Teachers	Incident IQ	16
Account Lifecycle Workflow	IC Scheduling N-Numbers (Additional Employee Accounts)	Incident IQ	16
WORKFLOWS – Internal (No IncidentIQ)			
Account Lifecycle Workflow	Contractor Teacher / Staff for IC Enterprise – C-Number Sponsorship — Sponsorship module; sensitive data stored in secure DB	Internal / MUNIS	16
Account Lifecycle Workflow	Lead Teacher SPED, Speech Language Pathology, Occupational Therapy (E9800s) — Currently managed via email and tracked in spreadsheet	Internal / MUNIS	16
Account Lifecycle Workflow	Itinerant Teachers — Secondary MUNIS data from HR staff file table	Internal / MUNIS	16
Account Lifecycle Workflow	Interim Principals, Assistant Principals, Counselors — MUNIS data from HR staff file table	Internal / MUNIS	16

Deliverable / Workflow	User Type / Description	Integration	Hours
Account Lifecycle Workflow	Gnet Teachers — MUNIS data from HR staff file table	Internal / MUNIS	16
ADDITIONAL SERVICES			
IncidentIQ Integration Design & Configuration			16
MUNIS Staff Import Job Update (SoA Migration)			24
Frontline Import Provisioning (Pre-Hire Accounts)			24
Canvas Export Provisioning (Staff & Pre-Hire to Canvas)			24
Total Defined Hours	232		

Total Defined Professional Services Hours: 232 hours

All line items above are included in the total.

7. Assumptions

The following assumptions govern the delivery of this engagement. Any deviation from these conditions may result in a change order, adjusted timeline, or additional cost.

7.1 Scope Limitations

- Any additional hardware and software purchases related to unforeseen items during the project are not included in this scope of work.
- Writing back to the HRMS or SIS is not included unless explicitly stated in the scope of work or use case sections.
- Account merging/splitting is not supported within this SOW (e.g., a temporary or sponsored account becoming a full-time account, or vice versa). Additional functionality can be addressed via a Change Order.
- Any items or functionality not included in this Statement of Work — including Connect Action Sets — are outside project scope and would require a separate SOW or change order, incurring additional costs.

7.2 Access and Timeliness

- The customer will provide timely access to all devices, facilities, systems/applications, and services necessary to complete the tasks in this scope of work. Failure to provide timely access will result in a change order and resetting of project timelines and anticipated go-live date.

7.3 Data Requirements

- Uniquely identifiable information must be populated within all applications in scope.
- All use cases, unless otherwise specified, will be built within production systems. Building in development or test environments is not supported under this scope and would require a change order.
- If complete production data is not available at the time of design, the solution will be built to adhere to defined business process rules. If production data does not meet defined conditions or formatting at the time of build, a change order will be required and the project timeline is at risk of delay.

7.4 Consulting Services and Data Exposure

- Identity Automation does not provide consulting services on source or destination systems for the purpose of creating queries or views. Any triggers (database views, CSV exports, SQL queries, etc.) required in the HR/SIS system must be created by the Customer or their system vendor at the Customer's expense.
- Identity Automation may consult on data to be included but will not own or be responsible for issues arising from suggestions made. Customers should validate with their respective vendors.
- Additional data introduced after the design phase may cause data issues. All data must be maintained in a consistent and reasonable manner. Changes to data formats or values that are not communicated to Identity Automation may incur additional costs or a change order.
- Changing data sources mid-project will constitute a change order and may result in additional costs.
- Identity Automation may request additional data as business logic requires. The Customer is expected to provide such data; otherwise the business logic will need to be revised.

7.5 Data Cleansing and Corrections

- Identity Automation will provide basic analysis and reports of source system data (upon Customer providing the data) identifying items requiring cleansing. The Customer is responsible for all actual data corrections. Data must be cleansed before automated synchronization can begin.

7.6 Acceptance Testing

- Customers will perform acceptance testing in advance of production rollout.
- Test cases will be written and provided by Identity Automation staff prior to completion. Successful completion of these test cases constitutes project completion.
- Identity Automation staff will conduct test cases with the Customer to assist in knowledge transfer and reliability testing. Customers will use these sessions to perform UAT for any further testing.
- Test users and groups MUST be provided prior to any testing. These must mimic all use cases (student, staff, and other user types). Failure to provide these may result in project timeline delays and inaccurate test results.
- Acceptance testing will be performed immediately after the solution is built, unit testing is complete, and log files have been provided.

7.7 Resource Allocation

- Identity Automation may allocate additional resources as deemed appropriate, provided such allocation does not cause production costs to exceed the amount agreed upon herein.

7.8 Change Management and Documentation

- Decisions by the Customer not to follow best practices will be documented and placed on the project RAID log.
- Functionality demos requested by the Customer will not exceed the time allotted for weekly progress checkpoint meetings.

7.9 Data Authority and Target Systems

- There should be no data elements with dual, competing sources of authority.
- This package includes the target systems indicated in this scope of work. Any change or addition to target systems may result in a change to package cost.
- Identity Automation engineers do not provide consulting or advice on DirSync, Azure AD Connect, or Entra ID. It is recommended to consult with a Microsoft engineer prior to disabling any of these tools to confirm migration completion and avoid negative repercussions. Please reference Microsoft documentation for proper procedures.

7.11 Sensitive Data Handling

- Data will be handled in a manner that secures user identity. From an Identity and Access Management perspective, only data used to make business decisions or required by systems in scope will be gathered.
- Sensitive data refers to information that is stored, processed, or managed by an individual or organization and is confidential — accessible only to authorized users with proper permissions. Unauthorized exposure of sensitive data could result in financial loss, security compromise, privacy violations, or competitive disadvantage.

- Identity Automation will not store passwords in plain text or produce lists or exports of plain text passwords under any circumstance.

7.12 Account Deletion and Risk

- Account deletions in any system are not included unless explicitly stated in the scope of work or use case sections.
- Accounts will not be deleted from RapidIdentity. Accounts created in RapidIdentity are tied to auditing information, and the platform does not natively expose a delete function to end users.
- Customers assume all risk for deletion of accounts in downstream systems, which may result in orphaned accounts no longer managed by RapidIdentity.
- Legal requirements for deletion of identity data may result in a change order, and the Customer will assume all associated risks.

7.13 Project Continuity and Delays

- Projects are designed to be executed continuously through to completion and production deployment once started.
- Any delay in project deployment may result in the reassignment of the Identity Automation engineer and potential rescheduling. Engineer availability requires a minimum of 30 days notice before an engineer can be rescheduled back onto the customer project.
- Availability may exceed 30 days during peak periods such as Summer, Winter Break, or Spring Break.
- Any project delays may introduce risk to originally agreed-upon go-live dates, including start of school.