ATLANTA PUBLIC SCHOOLS | Division of Information Technology



BUSINESS OWNER ONBOARDING GUIDE AND INTAKE CHECKLIST

GUIDE TO TECHNOLOGY INTAKE, SECURITY REVIEWS, AND CONTRACT APPROVALS

PREPARED BY: APS IT/PMO GOVERNANCE

Last updated: November 5, 2026

Contents

1. Welcome from IT Governance: Balancing Innovation and Protection 4
2. Business Owner Pre-Flight Checklist 4
3. What We Check and Why It Matters 4
   A. The SOC 2 Type II Report (The "Building Inspection") 4
      What It Is 4
      Why Do We Need It 4
      The Cloud Host Trap (AWS / Azure) 4
      What is a Bridge Letter 5
   B. The Memorandum of Understanding (MOU) and Contract 5
      What It Is 5
      Why Do We Need It 5
      What We Check For 5
   C. The Data Sharing Agreement (DSA) and Student Privacy Exhibits 5
      What It Is: 5
      Why Do We Need It: 5
      What We Check for When Student or Staff Data Is Involved: 5
   D. Hardware, Robotics, and STEM Lab Reviews 6
      What It Is 6
      Why Do We Need It 6
      What We Check For 6
4. How the Review Teams Support You 6
5. What Happens if a Vendor Cannot Meet Standards? (The Risk Acceptance Option) 6
6. Ready to Get Started? Next Steps for Business Owners 7
Appendix A. Business Owner Intake and Approval Checklist 8
   1. Clarify the Request 8
   2. Request the Vendor Documentation 8
Appendix A | Continued — Evaluate and Submit 9
   3. Prepare the Review Questions 9
   4. Submit Intake and Coordinate Reviews 9
Appendix A | Continued — Approval and Decision Log 10
   5. Confirm the Approved Path Before Purchase or Go-Live 10
   REVIEW / APPROVAL TRACKER 10
   OPEN ITEMS / NEXT ACTIONS 10

Appendix B. Acronyms and Abbreviations 11
Appendix C. Glossary of Terms 13

1. Welcome from IT Governance: Balancing Innovation and Protection

As a Business Owner, you are driving innovation to improve student outcomes and streamline operations.

The role of IT Governance is not to slow down your project or block releases. Our mission is to partner with you to balance efficiency, effectiveness, and compliance while protecting our 50,000+ students and staff members from cybersecurity threats, data leaks, and regulatory penalties under federal privacy laws (FERPA and COPPA).

To help us support your timeline and prevent administrative delays before purchase orders are cut, please submit your request through the IT PMO Project Intake Form. This ensures your project is assigned a tracking ID, evaluated by the right technical subject matter experts, and guided smoothly across the finish line.

2. Business Owner Pre-Flight Checklist

Before submitting your intake or sending documents to Procurement and Legal, use this checklist to gather the necessary vendor files:

- ☐ **VENDOR PROPOSAL / QUOTE / INVOICE:** Itemized list of all software licenses, hardware, routers, tablets, or services.
- ☐ **INDEPENDENT SECURITY AUDIT (SOC 2 Type II)**
  - An audit report from the last 12 months covering the vendor's actual software application.
  - If older than 90 days, request a signed "Bridge Letter" from the vendor.
    DATA SHARING AGREEMENT (DSA) / DATA SECURITY EXHIBIT: Required whenever student or employee names, IDs, grades, or rosters are shared.
- ☐ **MEMORANDUM OF UNDERSTANDING (MOU) / CONTRACT:** Standard district agreement establishing terms, scope, and service commitments.
- ☐ **HARDWARE and NETWORK SPECS (If purchasing physical devices/robots):** Confirmation of how the device connects (District Wi-Fi vs. Cellular SIM cards).

3. What We Check and Why It Matters

We know technical and legal paperwork can feel overwhelming. Here is a plain-language explanation of each key document, why IT Governance requires it, and what we are looking for on your behalf:

A. The SOC 2 Type II Report (The "Building Inspection")

What It Is: A formal, independent audit conducted by a licensed CPA firm that tests a vendor's internal security controls over a continuous 6- to 12-month period.

Why Do We Need It: Anyone can claim their software is secure. A SOC 2 Type II is the industry-standard "home inspection report" proving the vendor actually locks its digital doors, enforces strong passwords, and trains its staff.

The Cloud Host Trap (AWS / Azure): Many vendors say, *"We are secure because we host on Amazon Web Services (AWS)."* AWS only secures the physical data center and server power. If the vendor writes sloppy code, uses weak passwords, or lets unauthorized employees view student records, Amazon cannot stop them. The SOC 2 must cover the vendor's proprietary application, not just its cloud landlord.

What is a Bridge Letter: If a vendor's audit ended more than 90 days ago, a Bridge Letter is a signed note from its executive team confirming that its security practices have not changed since the last audit. If its audit hasn't happened yet or is scheduled for next year, the document is not valid for live data.

B. The Memorandum of Understanding (MOU) and Contract

What It Is: The primary legal agreement between the district and the vendor that outlines the scope of work, project goals, and legal responsibilities.

Why Do We Need It: It defines what the vendor will deliver, what it will cost, and who is responsible if something goes wrong.

What We Check For:

- ***Clear Project Scope:*** Ensuring the vendor only provides what was approved and preventing hidden costs or unvetted modules.
- ***Fixing Security Flaws:*** Enforcing concrete timelines for vendors to patch vulnerabilities (e.g., 72 hours for critical flaws) rather than vague promises to fix things "promptly."
- ***Quick Breach Notice:*** Requiring the vendor to notify the district within 48 hours if our data is ever compromised so we can protect our families and staff.

C. The Data Sharing Agreement (DSA) and Student Privacy Exhibits

What It Is: A specialized legal exhibit attached to the contract that strictly governs how student and employee data is handled, stored, and deleted.

Why Do We Need It: Federal laws (FERPA and COPPA) and Georgia state law (SDA) legally require the district to protect student education records from unauthorized access and commercial exploitation.

What We Check for When Student or Staff Data Is Involved:

- ***100% District Ownership:*** The district owns all data, records, and student work at all times.
- ***Strict AI Restrictions:*** Prohibiting the vendor from feeding student essays, test scores, or staff records—even if "de-identified"—into Artificial Intelligence (AI) or Large Language Models (LLMs) to train commercial tools.
- ***No Commercial Profiling or Ads:*** Banning vendors from tracking students, creating behavioral profiles, or selling data for advertising.
- ***Data Destruction (15 Days):*** Requiring the vendor to completely purge and delete all district records within 15 to 30 days when the contract ends and provide written proof of destruction.
- ***Secure Single Sign-On (SSO):*** Allowing staff and students to log in safely using their standard district credentials with Multi-Factor Authentication (MFA), rather than manually emailing class spreadsheets with student names and emails.

D. Hardware, Robotics, and STEM Lab Reviews

What It Is: A technical review of physical devices, sensors, and instructional robotics purchased for classrooms.

Why Do We Need It: Smart devices often contain hidden transmitters, cameras, and microphones that can disrupt our school Wi-Fi or create unmonitored security holes.

What We Check For:

- ***No Unmanaged Cellular Connections (eSIMs/4G):*** Hardware that connects to external cellular networks bypasses our district firewalls and web filters, meaning student web traffic and camera feeds are completely unmonitored.
- ***No Unmanaged Wi-Fi Routers:*** Vendors sometimes include private routers that create "rogue networks," interfering with classroom Wi-Fi and degrading network performance for nearby teachers.
- ***Zero Unauthorized Camera/Audio Telemetry:*** Ensuring cameras and microphones used on classroom robots do not stream live student video or audio back to third-party vendor servers without district authorization.

4. How the Review Teams Support You

You do not have to navigate this process alone. Several specialized departments collaborate to protect your project:

- **IT Governance and Security:** We evaluate technical risk, verify audit validity, inspect hardware, and ensure systems integrate cleanly with our enterprise tools.
- **Legal Counsel (Parker Poe):** Legal embeds our required Data Security Exhibits into vendor agreements, pushes back on high-risk vendor changes, and ensures the district is protected from liability.
- **Procurement:** Procurement ensures state purchasing rules are met and issues the Purchase Order (PO) once all governance, legal, and financial approvals are secured.
- **Your Responsibility:** As the Business Owner, you remain the ultimate authority on your program's goals. Always check in with Legal and IT Governance to confirm that vendor redlines do not compromise your timeline or scope.

5. What Happens if a Vendor Cannot Meet Standards? (The Risk Acceptance Option)

Sometimes a critical instructional tool or assessment is needed immediately, but the vendor does not yet hold a completed SOC 2 Type II audit or pushes back on standard contract terms.

When this happens, IT Governance will not simply reject your project and walk away. Instead, we outline two clear paths forward:

1. **Staged Non-Production Rollout (Recommended):** You can collaborate with the vendor on project planning, professional development, and interface setup using scrambled, synthetic, non-student test data while the vendor works to complete its security audit.

2. **Executive Risk Acceptance:** If your department must go live with district production records before an audit is completed, IT Governance will draft a formal Risk Acceptance Form. This form outlines the exact technical vulnerabilities, allowing your Cabinet-level Division Head to formally acknowledge and accept operational and financial responsibility on behalf of the division.

6. Ready to Get Started? Next Steps for Business Owners

1. Contact your Vendor: Request the vendor's current SOC 2 Type II report, itemized quote, and agreement terms.
2. Submit an Intake Ticket: Log into the IT PMO Project Intake Portal and submit your project details.
3. Collaborate and Deploy: IT Governance and Legal will review the files, incorporate our baseline exhibits, and clear your solution for a safe, successful rollout.

Appendix A. Business Owner Intake and Approval Checklist

WORKING COPY • Keep this checklist with the intake request, mark each action as complete, and record a date or N/A when an item does not apply.

Request / Project	_____	**Business Owner**	_____
Vendor / Solution	_____	**Department / School**	_____
Intake tracking ID	_____	**Target start date**	_____

How to use: Mark ☐ when completed; write N/A for nonapplicable items. Keep supporting documents with the intake. IT Governance, Legal, and Procurement conduct their own reviews and approvals.

1. Clarify the Request

Before contacting Procurement or submitting the intake ticket

Done	Business Owner action	Date / N/A
☐	Describe the business or instructional need, expected benefit, intended users, and proposed solution.	_____
☐	List the products, software modules, licenses, services, and physical devices within the requested scope.	_____
☐	Identify whether the solution will access APS student or staff records (e.g., names, IDs, grades, or rosters).	_____
☐	Identify planned logins, integrations, network connections, and any device cameras, microphones, or sensors.	_____

2. Request the Vendor Documentation

Collect these files before submitting the intake wherever applicable

Done	Business Owner action	Date / N/A
☐	Itemized vendor proposal, quote, or invoice covering licenses, hardware, and services.	_____
☐	Vendor contract or Memorandum of Understanding (MOU), including scope and service commitments.	_____
☐	Independent SOC 2 Type II audit from the last 12 months that covers the vendor's actual application—not only its cloud host.	_____
☐	Signed vendor Bridge Letter if the SOC 2 audit period ended more than 90 days ago.	_____
☐	Data Sharing Agreement (DSA) and Data Security Exhibit when student or employee information will be shared.	_____
☐	Hardware/network specifications for devices, robotics, routers, cellular SIM/eSIM connections, or wireless equipment.	_____
☐	Record the vendor contact who can answer security, technical, contract, and privacy questions.	_____

Appendix A | Continued — Evaluate and Submit

Use these prompts to prepare for review. Formal validation and contract decisions remain with the designated APS review teams.

3. Prepare the Review Questions

Document anything the vendor cannot answer or will not agree to

Done	Business Owner action	Date / N/A
☐	Check that contract scope, pricing, modules, deliverables, and service commitments match the proposed purchase.	_____
☐	Ask how the vendor handles critical security fixes and breach notifications; the guide cites 72-hour critical-fix and 48-hour breach-notice examples.	_____
☐	Identify where APS data is stored, who can access it, and how APS retains ownership of its records and student work.	_____
☐	Ask whether any student or staff data—including de-identified data—is used for AI/LLM training, profiling, or advertising.	_____
☐	Document how records will be deleted at contract end and how proof of destruction will be provided (the guide references 15–30 days).	_____
☐	Document district Single Sign-On (SSO), Multi-Factor Authentication (MFA), and planned data transfer or roster-sharing methods.	_____
☐	For hardware, identify unmanaged Wi-Fi or cellular connections and external transmission of camera/audio information.	_____

4. Submit Intake and Coordinate Reviews

Continue tracking after the initial ticket is filed

Done	Business Owner action	Date / N/A
☐	Submit the project description and collected vendor files through the IT PMO Project Intake Portal.	_____
☐	Record the assigned intake/tracking ID and share it with the appropriate project stakeholders.	_____
☐	Respond to questions and document requests from IT Governance and Security, Legal, and Procurement.	_____
☐	Review proposed vendor contract redlines with Legal and IT Governance for impacts to the program scope or timeline.	_____
☐	Track unresolved requirements, outstanding documents, and next actions until the reviewers confirm disposition.	_____

Reminder: A vendor-hosting provider's certification does not substitute for evidence about the vendor's own application. Use Appendix B for acronyms and Appendix C for term definitions.

Appendix A | Continued — Approval and Decision Log

5. Confirm the Approved Path Before Purchase or Go-Live

Business Owners coordinate the handoff; APS review teams make their required determinations

Done	Business Owner action	Date / N/A
☐	Verify that required IT Governance/Security and Legal reviews have been completed.	_____
☐	Confirm the required financial and procurement approvals are in place before Procurement issues a Purchase Order (PO).	_____
☐	Confirm solution readiness, documented responsibilities, and the approved timeline before deploying with live APS data.	_____
☐	If standards cannot be met, discuss the recommended non-production approach using synthetic/non-student data with IT Governance.	_____
☐	If live production use is essential before outstanding security requirements are met, route the formal Risk Acceptance Form through IT Governance for Cabinet-level Division Head acknowledgment.	_____

REVIEW / APPROVAL TRACKER

Review or decision	Status / date	Reference, decision, or follow-up
IT Governance / Security review	_____	_____
Legal / contract review	_____	_____
Procurement and Purchase Order	_____	_____
Risk acceptance, if applicable	_____	_____
Approved deployment / next step	_____	_____

OPEN ITEMS / NEXT ACTIONS

1. _____
2. _____
3. _____

Final reminder: Do not interpret a submitted intake ticket, a vendor promise, or an unapproved contract as authorization to use live district records.

Appendix B. Acronyms and Abbreviations

Acronym / Abbreviation	Full Name	Meaning / Use in This Guide
AI	Artificial Intelligence	Technology capable of performing automated analysis, learning, or content generation. The guide restricts vendors from using APS student or staff data to train commercial AI tools.
APS	Atlanta Public Schools	The district responsible for reviewing, approving, and governing technology solutions, contracts, data use, and security requirements.
AWS	Amazon Web Services	Cloud hosting provider referenced as an example. The guide explains that an AWS security audit does not replace an audit of the vendor's own application.
COPPA	Children's Online Privacy Protection Act	Federal privacy law referenced in connection with protecting student information.
CPA	Certified Public Accountant	Licensed accounting professional or firm that may conduct an independent SOC 2 Type II audit.
DSA	Data Sharing Agreement	Agreement governing how student or employee data is shared, handled, stored, protected, and deleted.
eSIM	Embedded Subscriber Identity Module	Digital cellular connectivity technology referenced in the review of hardware that may bypass district firewalls and web filters.
FERPA	Family Educational Rights and Privacy Act	Federal law protecting the privacy of student education records.
IT	Information Technology	APS technology function responsible for technology governance, security, infrastructure, integrations, and technical review.
LLM	Large Language Model	Type of artificial intelligence model. The guide prohibits unauthorized use of district data for training LLMs.
MFA	Multi-Factor Authentication	Security method requiring more than one verification factor to authenticate a user.
MOU	Memorandum of Understanding	Formal agreement defining terms, responsibilities, scope, and expectations between APS and another party.
PII	Personally Identifiable Information	Information that identifies or can be used to identify an individual.

Acronym / Abbreviation	Full Name	Meaning / Use in This Guide
PMO	Project Management Office	APS IT function responsible for project intake, governance, tracking, and coordination of technology requests.
PO	Purchase Order	Formal purchasing document issued by Procurement after required governance, legal, and financial approvals are completed.
SIM	Subscriber Identity Module	Cellular connectivity component used by devices. The guide requires review of devices using SIM cards that may bypass APS network controls.
SOC 2 Type II	System and Organization Controls 2 Type II	Independent audit report evaluating a vendor's internal security controls and their operating effectiveness over a defined period.
SSO	Single Sign-On	Authentication method that allows APS staff and students to access applications using district credentials instead of separate vendor-managed credentials.
STEM	Science, Technology, Engineering, and Mathematics	Used in reference to instructional labs, robotics, sensors, and technology equipment requiring technical review.
Wi-Fi	Wireless Networking	Wireless connectivity technology referenced in the review of routers, devices, and potential rogue networks.

Appendix C. Glossary of Terms

Term	Definition / Application in This Guide
Business Owner	APS individual or department responsible for the business need, goals, scope, and operational use of a proposed technology solution.
Bridge Letter	Signed vendor document used when the vendor's SOC 2 Type II audit period ended more than 90 days earlier. It confirms whether material security practices have changed since the last audit.
Cloud Host	Third-party provider that supplies hosting infrastructure, such as AWS or Azure. The guide explains that the cloud host's security controls do not replace an audit of the vendor's own software.
Commercial Exploitation	Unauthorized use of student or staff information for commercial gain, including selling data, advertising, or creating commercial profiles.
Commercial Profiling	Use of information to create behavioral or commercial profiles about students or staff. The guide prohibits vendors from using APS data for this purpose.
Contract	Legal agreement defining the services, obligations, responsibilities, pricing, security requirements, and other terms between APS and a vendor.
Data Destruction	Permanent deletion or purge of district records after a contract ends. The guide requires vendors to provide written proof that required destruction has occurred.
Data Security Exhibit	Contractual document establishing specific requirements for protecting, handling, accessing, retaining, and deleting district data.
De-Identified Data	Information from which direct identifying information has been removed. The guide states that de-identified student or staff data may not be used to train commercial AI or LLM systems.
District Production Data	Actual APS student, employee, operational, or other live district records used in production environments, as opposed to synthetic test information.
Hardware Review	Technical assessment of physical devices, sensors, robotics, routers, and other equipment to determine how they connect to APS networks and whether they create security risks.
Independent Security Audit	Security review conducted by an independent third party to verify a vendor's controls rather than relying solely on the vendor's own statements.
Intake Form / Intake Ticket	Formal submission used to initiate APS review of a proposed technology product, service, hardware purchase, or project.
Legal Counsel	Legal reviewers responsible for evaluating agreements, incorporating required data-security provisions, reviewing vendor redlines, and protecting APS from contractual liability.

Term	Definition / Application in This Guide
Live Data	Actual APS production information, including student or staff records, rather than synthetic or test data.
Non-Production Environment	Development, test, training, staging, or other environment that does not use live APS production data.
Pre-Flight Checklist	Document checklist Business Owners use before submitting a project for governance, security, legal, and procurement review.
Procurement	APS function responsible for ensuring purchasing requirements are satisfied and issuing Purchase Orders after required approvals are complete.
Project Intake	Formal process through which proposed APS technology projects and purchases are submitted for review, tracking, governance, security, and approval.
Redline	Proposed change, deletion, or revision to contract language made during negotiations between APS and a vendor.
Risk Acceptance	Formal process through which identified risks are documented and acknowledged when a vendor cannot meet standard APS requirements and leadership wishes to proceed.
Risk Acceptance Form	Formal document describing identified technical, operational, or compliance risks and recording leadership's decision to accept those risks.
Rogue Network	Unauthorized or unmanaged wireless network created inside the APS environment that may interfere with district Wi-Fi or bypass approved security controls.
Security Breach	Unauthorized access, compromise, disclosure, or loss involving district systems or data. The guide references a 48-hour vendor notification requirement.
Security Control	Technical, administrative, or operational safeguard used to protect systems, users, and data from unauthorized access or security threats.
Staged Non-Production Rollout	Approach that allows project planning, professional development, configuration, or interface setup to proceed using synthetic or non-student test data while security requirements remain unresolved.
Student Education Records	Student records protected under FERPA and subject to APS privacy, security, and data-handling requirements.
Subject Matter Expert	Individual with specialized technical, security, legal, procurement, or operational expertise who supports review of a proposed technology solution.
Synthetic Data	Artificially created test information that does not contain real student, employee, or protected APS information.
Telemetry	Data automatically collected and transmitted by a device, including audio, video, camera, sensor, or operational information.
Third-Party Vendor	External company or service provider supplying technology, hardware, applications, hosting, or related services to APS.

Term	Definition / Application in This Guide
Unauthorized Camera/Audio Telemetry	Transmission of student video or audio from devices to external vendor systems without appropriate APS authorization.
Unmanaged Cellular Connection	Device connection using cellular technology such as eSIM or 4G that bypasses APS firewalls, web filters, or other network controls.
Unmanaged Wi-Fi Router	Wireless router installed or operated outside APS network management and security controls.
Vendor Proposal / Quote / Invoice	Vendor documentation showing the products, licenses, hardware, services, quantities, or costs included in a proposed purchase.