BY ORDER OF THE COMMANDER
AIR EDUCATION TRAINING COMMAND

AIR EDUCATION AND TRAINING COMMAND MANUAL 90-7001

29 DECEMBER 2025

Special Management

AETC STUDENT AND LEARNING DATA STANDARDS

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: This publication is available for downloading or ordering on the e-Publishing website at www.e-Publishing.af.mil

RELEASABILITY: There are no releasability restrictions on this publication

---

OPR: AETC/CDO

Certified by: AETC/A3/6

Pages: 39

This publication implements Air Force Policy Directive (AFPD) 90-70, *Enterprise Data Management* and Department of the Air Force Instruction (DAFI) 90-7001, *Enterprise Data Sharing and Data Stewardship*. It provides guidance on the development and implementation of data standards and governance structures for Air Education and Training Command (AETC), ensuring alignment with Department of the Air Force (DAF) policy for Learning Management Systems (LMS), Student Information Systems (SIS), Human Performance Management Systems (HPMS), Training Management Systems (TMS), Learning Record Stores (LRS), Competency-Based Education Systems (CBES), Extended Reality (XR) technologies, and all other information systems (IS) that handle student and learning data across the organization. This publication applies to all AETC civilian employees and uniformed members of the Regular Air Force, the Air Force Reserve, the Air National Guard (ANG), government-contracted personnel assigned to AETC, and its associated information, information systems, and cyberspace and information technology (C&IT) infrastructure within AETC's information technology (IT) Portfolio and Enterprise Data Management (EDM). This publication does not apply to the United States Space Force (USSF). **Exception:** AETC Personnel under the operational control of a non-AETC agency, or school, or using other IS that handle student and learning data which are acquired, managed, and sustained by a non-AETC organization, must comply with the guidance and requirements established by contract, memorandum of agreement (MOA), memorandum of understanding (MOU), or training affiliation agreement (TAA) between those agencies or schools. These agencies and schools include, but are not limited to: non-AETC DAF organizations, Department of the Army, Department of the Navy, Department of Defense (DoD), Defense Health Agency, and the Medical Education Training Center. Ensure all records generated as a result of processes prescribed in this

publication adhere to Air Force Instruction (AFI) 33-322, *Records Management and Information Governance Program*, and are disposed in accordance with the Air Force Records Disposition Schedule, which is located in the Air Force Records Information Management System. Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the DAF Form 847, *Recommendation for Change of Product*; route DAF Forms 847 from the field through the appropriate functional chain of command. This publication may be supplemented at any level, but all supplements must be routed to the OPR of this publication for coordination prior to certification and approval. To the extent its directions are inconsistent with other AETC directive publications, including AETC supplements to higher headquarters publications, the information herein prevails. To the extent its directions are inconsistent with higher headquarters (e.g., Air Force and Department of Defense) directive publications; the directives in the higher headquarters publication prevails and relief for non-compliance (a waiver) must be granted before deviating from established standard, The authorities to waive requirements in this publication are identified with a Tier ("T-0, T-1, T-2, T-3") number following the compliance statement. Submit requests for waivers through the chain of command to the appropriate Tier waiver approval authority, or alternately, to the publication OPR for non-tiered compliance items. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the DAF.

Chapter 1

OVERVIEW

1.1. Background.

1.1.1. This manual establishes a standardized approach for managing, governing, and integrating data within all student and learning information systems across the organization. There is a proliferation of publications, manuals, policies, and standards related to data governance and management. Many of these documents contain broad statements such as, "data should be governed and protected while remaining accessible." While intended to establish a guiding principle, these statements lack the practical implementation details or an established framework necessary for effective data governance.

1.1.2. As AETC has evolved, multiple units deployed student and learning-related IT systems without centralized guidance, as no unified framework for data governance, interoperability, and security previously existed. The absence of standardized approaches resulted in standalone deployments, data silos, network integration challenges, and inconsistencies in data handling across different platforms. The net result is an AF-wide inability to assess real-time feedback on student/syllabi/training performance and incorporate big-data techniques to affect improvements and efficiency in training.

1.1.3. AETC student and learning data standards provide structured guidance to ensure all systems handling student and learning data adhere to command-wide best practices, DoD/AF regulations, and mission-aligned objectives as outlined in DoD Instruction (DoDI) 1322.26, Distributed Learning and the Total Learning Architecture Standards. To ensure AETC effectively leverages its learning and force development data as a strategic asset, all AETC IT systems and programs that generate student and learning data must be designed and operated to make their data readily available to the enterprise in alignment with VAULTIS (Visible, Accessible, Understandable, Linked, Trustworthy, Interoperable, and Secure) principles. This includes implementing standardized data formats, robust metadata management, secure data sharing mechanisms, and quality assurance processes as detailed throughout this manual. Rather than mandating retroactive compliance for existing systems, this manual directs standards for future acquisitions and system integrations while providing strategic goals for existing systems. Retroactive implementation of these standards will be evaluated on a case-by-case basis, considering the operational impact of existing nonstandard data. Specific implementation guidance to support these objectives is provided in **Chapter 3** and **Chapter 4**, ensuring new system deployments clearly align with these standards and contribute to a unified data strategy.

1.1.4. The purpose of this manual is not to create a rigid, static standard that must receive continuous approval from leadership. Instead, it is designed to solve real-world operational challenges by providing practical guidance that evolves with technological advancements and mission requirements, while supporting compliance with Air Force records-management standards established by AFI 33-322. Given the rapid pace of technological and operational change, detailed and tactical-level guidance are maintained separately within the Technical and Operational Practices and Standards (TOPS) resource library, which includes supplemental documents such as the Technical Data Standards Guide (TDSG), Implementation Guide, and Compliance Programs. The TOPS resources are managed by the Command Data Officer

(CDO) and supported by established governance structures including the Enterprise Architecture Working Group (EAWG), Data Governance Working Group (DGWG), and Data Stewardship Framework defined in this manual. This approach ensures responsiveness and compliance at speed and scale, enabling timely updates without compromising the enduring policies and oversight provided by this manual.

1.2. Why Standardized Data Practices Are Necessary.

1.2.1. Historically, units have purchased, configured, and deployed systems independently, leading to:

1.2.1.1. Lack of interoperability between systems, requiring custom integrations or manual data transfers.

1.2.1.2. Challenges in tracking personnel training and performance across systems due to inconsistent data structures and reporting methodologies.

1.2.1.3. Inadequately defined data transition procedures when contracts end, causing units difficulty in reliably accessing and retaining mission-critical training and performance records.

1.2.1.4. Standalone deployments that later require complex retrofitting to meet network integration requirements.

1.2.1.5. Proliferation of multiple learning systems with redundant and duplicative capabilities.

1.2.2. To mitigate these challenges, this manual establishes mandatory guidelines for how IT systems handling learning-related data must be developed, deployed, integrated, and managed within the organization's IT ecosystem.

1.3. Objectives of this Standard.

1.3.1. Enable Full System Interoperability. Ensure all student and learning information systems exchange data seamlessly using standardized frameworks such as: Experience Application Programming Interface (xAPI), Sharable Content Object Reference Model (SCORM), Learning Tools Interoperability (LTI), and *OneRoster* (see **Attachment 1**), as directed by DoDI 1322.26 and *Total Learning Architecture (TLA) Standards*.

1.3.2. Strengthen Data Governance. Establish clear ownership, stewardship, and accountability for managing training and performance-related data across the command in alignment with AFPD 90-70 and DAFI 90-7001.

1.3.3. Ensure Long-Term Data Access and Security. Implement structured data retention policies to prevent the loss of training records due to vendor changes or system migrations as required by AFI 33-322.

1.3.4. Enhance Data Security and Privacy. Implement robust security controls in accordance with DoDI 8510.01, *Risk Management Framework for DoD Systems,* AFI 17-101, Risk Management Framework (RMF), AFI 17-130, *Cybersecurity Program Management*, and AFI 33-332, *Air Force Privacy and Civil Liberties Program* to protect sensitive training data and Personally Identifiable Information (PII).

1.3.5. Enable Integration of Innovative Solutions. Ensure standalone and innovative pilot systems implement data standards that facilitate eventual integration with enterprise systems. This approach balances the AETC innovation imperative with effective enterprise data management, allowing units to develop and test new solutions while preserving technical compatibility for scaling successful innovations across the command.

1.3.6. Reduce the AETC Application Footprint. Ensure new applications are formally reviewed by an EAWG to prevent duplication of capabilities into the AETC landscape.

1.4. AETC Standard. This AETC manual applies to all student and learning data and all IT systems that collect, process, store, and/or transmit student and learning data. This includes systems used to support training, competency tracking, mission qualification, human performance monitoring, and immersive learning experiences across military, civilian, and contractor personnel. By defining a clear scope, this manual ensures consistent application of data governance principles across all systems handling student and learning data. All covered systems and personnel involved in their design, deployment, integration, or administration (including data governance, system administration, cybersecurity, and training operations) must adhere to these data standards to ensure compliance with DoD/AF regulations, interoperability, and mission readiness. Legacy systems that do not yet meet these standards may follow a phased transition plan toward compliance when it is determined that the cost of non-compliance is greater than the cost to modify the legacy system. This is not mandatory but will be determined on a case-by-case basis. Custom-built applications are also expected to meet minimum compliance requirements to ensure interoperability across platforms. In certain cases, temporary waivers may be granted for mission-critical systems that require immediate deployment. However, a plan for achieving compliance must be submitted and approved within a timeframe determined by the appropriate authority. AETC recognizes implementing these standards across diverse existing systems presents practical challenges. While compliance with these standards is mandatory, a separate *Implementation Guide,* maintained and accessible by contacting the OPR at: **aetcdataoffice@us.af.mil**, will establish detailed implementation timelines, phased approaches for different system categories, and a formal exemption process for systems where immediate compliance is not technically or financially feasible. Units should continue planning for eventual compliance while awaiting this guidance.

Chapter 2

ROLES AND RESPONSIBILITIES

2.1. AETC Leadership.

2.1.1. The Commander AETC (COMAETC) will:

2.1.1.1. Provide strategic direction and leadership for data management initiatives across AETC.

2.1.1.2. Establish command-wide priorities for leveraging student and learning data as a strategic asset to enhance training effectiveness, operational readiness, and decision-making capabilities.

2.1.1.3. Foster a data-informed culture that supports the AETC mission through collaborative networks and the adoption of enterprise data standards.

2.1.2. The AETC Deputy Commander (DCOM) will:

2.1.2.1. Serve as the approval authority for all IT and data management investments for the command.

2.1.2.2. Provide executive-level oversight of data governance activities, ensuring alignment with AETC strategic objectives and DoD data policies.

2.1.2.3. Establish accountability for effective resource allocation supporting the command's data management initiatives and strategic priorities.

2.1.3. The AETC Director, Operations and Communications (AETC/A3/6) will:

2.1.3.1. Provide strategic oversight of digital transformation efforts for all systems/applications supporting the AETC mission.

2.1.3.2. Serve as the command's IT Portfolio Management decisional authority, as delegated by AETC DCOM to AETC/A3/6.

2.1.3.3. Serve as the certification authority for AETC data management instructions, manuals, and/or guides, to ensure compliance with, or meet the intent of, higher headquarters publications or initiatives.

2.1.4. The AETC Deputy Director for Operations and Communications and 17X Functional Manager will:

2.1.4.1. Report to and advise the AETC DCOM on IT and data management resource implications of strategic planning decisions.

2.1.4.2. Represent AETC equities in AF-level IT governance bodies (e.g., Enterprise Information Technology Council, Program Review Board).

2.1.4.3. Ensure alignment with Air Force Deputy Chief of Staff, Manpower and Personnel (AF/A1) and Assistant Secretary of the Air Force for Financial Management and Comptroller (SAF/FM) IT portfolio requirements.

2.1.4.4. Through AETC/A6CS, serve as the IT Portfolio Manager, responsible for day-to-day operational management of the command’s IT portfolio.

2.1.5. The AETC Chief Learning Officer (CLO) will:

2.1.5.1. Advise the AETC CDO on IT and learning best practices and implications of strategic planning decisions.

2.1.5.2. Collaborate within the DoD to establish connections between research, learning environments, and operations to influence data best practices.

2.1.6. AETC IT Data and Oversight Governance (IDOG). The IDOG, established under the AETC corporate structure, provides the AETC DCOM the authority and oversight to effectively manage the IT portfolio and EDM within AETC. The IDOG will:

2.1.6.1. Hold meetings on a quarterly basis or as requested by IDOG members. IDOG members include representatives from: AU, AFAC, 19 AF, 2 AF, 502 ABW, AETC Directors, CDO, Chief Technology Officer (CTO), CLO, IT investment owners/program managers, and other invited subject matter experts as required.

2.1.6.2. Provide strategic direction through the IDOG evaluation process, establishing standards, and prioritizing IT and data investments, while ensuring that they align with the command's overall mission goals and objectives.

2.2. AETC Data Stewardship. Note: Specific responsibilities for each member of the AETC Data Team, listed below, can be found in the *AETC Data Stewardship Framework*, a document maintained and accessible by contacting the OPR at: **aetcdataoffice@us.af.mil**.

2.2.1. Command Data Officer (CDO).

2.2.1.1. The AETC CDO, and by extension the AETC Data Team, will act with authority and accountability for management of AETC mission data. Per DAFI 90-7001, MAJCOM Data Officers, in this case the AETC CDO, will provide subject matter expertise to assist SAF/CO with the drafting of policies and guidance and represent AETC in SAF EDM bodies to ensure understanding and consideration of the unique requirements of learning data.

2.2.1.2. The AETC CDO will participate in the DAF data governance as appointed to represent the interest of AETC's EDM and data sharing.

2.2.2. Mission Data Steward (MDS).

2.2.2.1. MDSs will align to mission areas within AETC. Key examples include broad mission areas such as: recruiting, technical training, flying training, learning services, etc., as well as focused mission capabilities such as: DAF Learning Record (DAFLR), Tech Training Management System (TTMS), etc., as appropriate. MDSs will provide subject matter expertise support from a mission area perspective.

2.2.2.2. MDSs will understand the mission, their systems/applications, and the data within and how the data supports the mission. MDSs will support the establishment of protection, sharing, and governance guidelines; maintain data names, definitions, data integrity rules, and domain values; ensure compliance with the appropriate level (e.g., DoD, DAF, AETC) legal and policy requirements, and conformance to data policies and standards; ensure application of appropriate security controls; and analyze and improve data quality.

2.2.3. Service Data Manager (SDM).

2.2.3.1. The purpose of the SDM is to support governance of their project or programs (project and programs will be referred to as 'project' henceforth) to ensure alignment with existing policy and strategies. These individuals will be system owners, program managers, project managers or someone assigned by these individuals. SDMs report up to the MDS and work alongside the Technical Data Custodians (TDC).

2.2.3.2. SDMs operate at the tactical level of the Air Force's Data Stewardship model. According to the *DoD Data Stewardship Guidebook*, SDMs: "implement enterprise and domain-specific data management policies and maintain the quality of the data within their scope of responsibility."

2.2.4. Technical Data Custodian (TDC).

2.2.4.1. AETC has created the role of TDC specifically to address the technical aspect of data management. These individuals could be system/application database engineers, administrators, system analysts, etc.

2.2.4.2. TDCs provide subject matter expertise from the information system perspective. TDCs have a stake in the data generated, processed, or transmitted by the AETC mission systems, and represent their unit/mission system. The TDCs operate at the tactical level of the DoD's Data Stewardship model and are mission system experts. A TDC aligns to the IT support of an information system and the duties performed are typically part of the system support contract.

Chapter 3

DATA REQUIREMENTS FOR IT SOFTWARE

3.1. Principle Overview. This section establishes the core guiding principles and compliance requirements for the implementation, management, and governance of all AETC information systems handling student and learning data within the military training and development context. These principles form the foundation for responsible system management throughout the command, ensuring data security, interoperability, and alignment with DoD/AF policies, supporting mission readiness, command-wide system integration, and regulatory compliance. By adhering to these principles, organizations can enhance data-driven decision-making, streamline training operations, and ensure long-term system sustainability.

3.2. Guiding Principles. The following five core principles define the framework for all student and learning information systems within the organization:

3.2.1. Data as a Strategic Asset.

3.2.1.1. All accessions, learning, and human performance data must be managed as a critical strategic asset. **(T-2)**

3.2.1.2. System owners and data stewards must ensure data accuracy, accessibility, and usability to support operational and decision-making processes. **(T-2)**

3.2.1.3. **Example Application:** Training records must be structured to allow seamless retrieval for performance tracking, certification renewals, and readiness reporting.

3.2.2. Interoperability and Standardization.

3.2.2.1. All student and learning information systems must support interoperability through industry-standard frameworks and protocols as specified in DoD and AF technical guidance. Current approved standards include: xAPI, SCORM, cmi5, LTI, and other frameworks identified in DoDI 1322.26. **(T-2)**

3.2.2.2. Systems should consider cmi5 capabilities for future implementations, as the standard provides enhanced content launch, tracking, and security features beyond traditional SCORM.

3.2.2.3. Systems must integrate with other organizational IT platforms to support comprehensive data management and exchange. **(T-2)**

3.2.2.4. **Example Application:** A learning management platform must automatically transmit course completion data to student record systems rather than requiring manual data entry.

3.2.3. Data Privacy Compliance.

3.2.3.1. Role-based access controls (RBAC) and multi-factor authentication (MFA) must be implemented to protect sensitive training and personnel data. **(T-2)**

3.2.3.2. **Example Application:** A system tracking physical fitness data must implement encryption and access restrictions to ensure compliance with data privacy policies per AFI 33-332.

3.2.4. Long-Term Data Retention and Accessibility.

3.2.4.1. Training and competency data must be stored securely and remain accessible beyond contract/vendor transitions to prevent the loss of mission-critical records. **(T-2)**

3.2.4.2. Data must be stored in structured formats (e.g., JavaScript Object Notation (JSON), Extensible Markup Language (XML), Comma-Separated Values (CSV)) when systems are decommissioned or data from the source system needs to be archived in an AETC data storage to allow seamless migration to new systems without significant reformatting. **(T-2)**

3.2.4.3. The EAWG will publish a JSON format for data archival. **(T-2)**

3.2.4.4. **Example Application:** When a training system is decommissioned, all training records must be exported and migrated to the next authorized system before shutdown, in accordance with AFI 33-322.

3.2.5. System Lifecycle Management and Avoiding Standalone Deployments.

3.2.5.1. All student and learning information systems, including those acquired through external vendors or integrated from existing systems, must undergo command IDOG review before deployment to prevent unauthorized, standalone applications. **(T-2)**

3.2.5.2. Systems must be planned with long-term integration in mind and not deployed as temporary workarounds to bypass IT approval processes. Integration planning should consider existing enterprise architecture and leverage already deployed systems when feasible. **(T-2)**

3.2.5.3. **Example Application:** An immersive training technology must be designed with network integration from the start rather than deployed as an isolated system with no enterprise connectivity.

3.3. Compliance Requirements. All student and learning information systems must comply with the applicable DoD and AF policies to ensure cybersecurity, data integrity, interoperability, and governance. In cases where no specific DoD and AF policy exists for a given system or functionality, the program office must consult with the AETC CDO to establish appropriate guidelines and ensure compliance with broader principles of security and interoperability. This consultation process should be documented and the resulting guidelines included in the system's documentation.

3.3.1. Mandatory Compliance Regulations and Directives. **Table 3.1** highlights key directives and their specific compliance requirements as they apply to student and learning information systems.

Table 3.1. Compliance Regulations and Directives.

Regulation/Directive	Key Compliance Requirements
DoDI 1322.26, *Distributed Learning*	Mandates interoperability standards (SCORM/xAPI) for learning systems.
DoDI 8510.01, *Risk Management Framework for DoD Systems*	Establishes the DoD approach to cybersecurity risk management.

AFPD 90-70, *Enterprise Data Management*	Requires standardized data governance across all enterprise systems.
DAFI 90-7001, *Enterprise Data Sharing and Data Stewardship*	Establishes data stewardship roles and mandates structured data sharing across the enterprise.
AFI 17-130, *Cybersecurity Program Management*	Establishes management controls and procedures for cybersecurity programs.
AFI 33-322, *Records Management and Information Governance Program*	Requires secure data retention, archiving, and proper disposal of training records.
AFI 33-332, *Air Force Privacy and Civil Liberties Program*	Ensures protection of PII in training systems.

3.3.2. System Compliance Checklist. While general IT requirements are addressed in broader AETC IT/IDOG guidance, the following requirements (see **Table 3.2**) are highlighted in this manual for their specific implications for student and learning data management. These requirements complement and do not supersede existing IT directives. Before implementation, all student and learning information systems must meet the following compliance requirements, exceptions will be requested forwarded to the DGWG and IDOG for approval/disapproval prior to deployment:

Table 3.2. System Data Compliance Checklist.

Requirement	Criteria
Interoperability	Must support industry-standard learning technology integration frameworks such as SCORM, xAPI, or other DoD-approved standards as specified in current technical guidance. **(T-2)**
Security	Must adhere to DoD cybersecurity policies (e.g., AFI 17-130) with specific attention to learning data protection requirements. **(T-2)**
Data Sharing	Must allow structured exports for reporting and analytics to support enterprise-wide data utilization. **(T-3)**
User Authentication	Must support Common Access Card (CAC) login or DoD-approved authentication methods to maintain data access accountability and traceability. **(T-2)**
Governance	Must have assigned data stewards responsible for maintaining data integrity and ensuring compliance with data standards. **(T-3)**
Lifecycle Planning	Must have a decommissioning and data migration strategy before system shutdown to prevent loss of valuable training and performance data. **(T-3)**

3.4. Ensuring Accountability in System Deployment. To ensure compliance, all newly deployed IT systems must adhere to the following three-phase approval process before full operational integration:

3.4.1. Phase 1: Pre-Deployment Review.

3.4.1.1. Submit a System Integration Plan for IT and cybersecurity review. **(T-2)**

3.4.1.2. Identify compliance gaps and required security modifications. **(T-3)**

3.4.1.3. Perform a sandbox deployment to test interoperability with existing platforms. **(T-3)**

3.4.1.4. Data Flow/Architecture Diagrams: Diagram showing data movement across systems, transformations, and storage; useful for assessing latency and integration. **(T-2)**

3.4.1.5. Entity-Relationship Diagram: Visual representation of entities and their relationships, showing how tables connect via keys. **(T-2)**

3.4.1.6. Data Dictionary/Schema Documentation: List tables, fields, data types, and descriptions to define the structure and purpose of each data element. **Note:** A comprehensive listing of key data elements is provided in **Attachment 2**. **(T-2)**

3.4.1.7. Sample Datasets: Anonymized, representative data samples used to validate structure, completeness, and content alignment. **(T-2)**

3.4.1.8. Data Lineage/Source Mapping: Details how data flows from source systems through transformations to final outputs, including dependencies. **(T-2)**

3.4.1.9. Logical Data Model: High-level model defining entities, relationships, and business context independently of implementation. **(T-2)**

3.4.1.10. Physical Data Model: Detailed schema showing tables, data types, constraints, and physical structure of how data is stored. **(T-2)**

3.4.1.11. Metadata and Tagging Standards: Documentation of classification, business metadata, and tagging conventions for cataloging and discoverability. **(T-2)**

3.4.1.12. Data Quality Plan: Outlines rules, validation logic, and completeness thresholds, along with known data issues or limitations. **(T-2)**

3.4.1.13. Glossary/Business Terms: Defines business terms, metrics, and concepts to promote semantic consistency across the organization. **(T-2)**

3.4.1.14. Data Classification and Sensitivity Matrix: Indicates regulated fields (e.g., PII). **(T-2)**

3.4.1.15. Access Control Requirements: Specify user roles, access permissions, and authentication methods required for secure data access. **(T-2)**

3.4.1.16. Audit and Logging Specifications: Describe how user activity, data changes, and access logs must be captured and monitored. **(T-2)**

3.4.1.17. Application Programming Interface (API) Specifications/ETL Mapping: Outline available APIs or Extract, Transform, Load (ETL) pipelines, including input/output formats, authentication, and refresh schedules. **(T-2)**

3.4.1.18. Deployment Checklist: Checklist to verify readiness of data components, including Quality Assurance signoff, governance approvals, and risk reviews. **(T-2)**

3.4.1.19. Monitoring and Alerting Plan: Define metrics, thresholds, and response plans for data quality, pipeline failures, and system health. **(T-2)**

3.4.2. Phase 2: Deployment Implementation and Validation.

3.4.2.1. System Data Stewards will lead the initiative to integrate with mandatory enterprise systems as defined by the EAWG. **(T-3)**

3.4.2.2. System Data Stewards will coordinate security validation testing with the CDO to ensure data security compliance. **(T-3)**

3.4.2.3. CDO will provide training for system administrators, data stewards and data owners to enforce governance policies. **(T-3)**

3.4.3. Phase 3: Post-Deployment Monitoring and Governance.

3.4.3.1. The DGWG will establish recurring data audits to verify compliance with retention policies and brief results to the IDOG quarterly. **(T-2)**

3.4.3.2. System Data Stewards will ensure that automated monitoring systems are in place to ensure continued data integrity. **(T-3)**

3.4.3.3. The CDO and IT Portfolio Management will document lessons learned and apply findings to future deployments. **(T-3)**

3.4.4. Testing Requirements.

3.4.4.1. All system integrations must be tested in a sandbox environment before production deployment. **(T-3)**

3.4.4.2. Testing must include data validation, security checks, and performance monitoring to verify system functionality. **(T-3)**

3.4.4.3. Interoperability failures must be documented with corrective action plans before system go-live. **(T-3)**

3.4.4.4. **Example Application:** Before integrating a student information system with a new learning management system, a test environment must be used to verify data consistency and reporting accuracy before implementation. The organization responsible for managing the target production environment is responsible for providing and maintaining this sandbox. The program office, in coordination with relevant stakeholders (e.g., functional users, system administrators), facilitates the testing process.

3.4.5. XR Technology Data Standards. The specific data standards for XR technologies are currently under development, pending the publication of the *AETC XR Policy*. This section outlines the intended direction and will be updated to reflect the finalized policy. Interim guidance will be provided as available by the OPR.

3.4.5.1. For XR technologies used in training environments, these technologies must capture standardized learning experience data including user interactions, assessment results, completion status, and learner performance metrics relevant to the training objectives (e.g., specific metrics to be defined in system implementation guides) to enable meaningful analysis. **(T-2)**

3.4.5.2. XR technologies, whether implemented as networked or standalone solutions, must structure captured data using xAPI statements or other approved formats to ensure compatibility with learning record stores and analytics systems. **(T-2)**

3.4.5.3. Training data from XR technologies containing mission-specific content must be properly classified and handled according to appropriate security requirements based on the sensitivity of the simulated scenarios. **(T-2)**

3.4.5.4. Example Application: A VR flight simulation technology must record standardized performance data that can be analyzed alongside data from other training modalities to assess overall pilot competency development.

Chapter 4

DATA MANAGEMENT

4.1. Standards. This section aligns with AETC's Data and Analysis Virtual Ecosystem (DAVE), which provides a governed framework to transform mission data into trusted, reusable assets that fuel data-informed decisions at speed and scale. The standards outlined here support DAVE's objectives of delivering actionable insights through enterprise data management and advanced analytics.

4.2. Data Definition and Modeling.

4.2.1. Data models (conceptual, logical, physical) must be developed and maintained by the CDO and approved by the EAWG for critical AETC data assets to ensure common understanding and facilitate integration. **(T-2)**

4.2.2. Modeling standards, including naming conventions and use of class words, must be established and promulgated by the CDO and approved by the EAWG to ensure consistency across IT systems. **(T-2)**

4.2.3. Authoritative reference data sources must be identified, managed, and made accessible by the CDO and approved by the IDOG after recommendation from the Data Connections Working Group (DCWG). **(T-2)**

4.3. Metadata Management.

4.3.1. Metadata (business, technical, operational) is critical for making data VAULTIS and will be audited by the CDO for compliance. Audits will be briefed regularly to the IDOG. **(T-2)**

4.3.2. An *AETC Metadata Template* must be completed for each data set created following the guidelines in the *AETC Metadata Standard*, maintained and accessible by contacting the OPR at: **aetcdataoffice@us.af.mil**. **(T-3)**

4.3.3. The Mission Data Steward will ensure the *AETC Metadata Template* is completed and confirm metadata accuracy and completeness for data within their domains. **(T-3)**

4.3.4. The CDO must establish and maintain a command Data Catalog to inventory and describe key data assets. Data Catalog implementation must leverage standardized Data Standards Objects through enterprise data integration platforms to ensure consistent metadata structure and governance across systems while maintaining platform agnosticism. **(T-2)**

4.3.5. Metadata standards, including requirements for definition, lineage, quality rules, and security/privacy tagging, must be defined and enforced by the CDO and approved by the IDOG after a recommendation from the DGWG.

4.4. Data Collection and Creation.

4.4.1. Data must be collected electronically at the point of creation whenever feasible. **(T-3)**

4.4.2. Data pedigree (origin, lineage) must be maintained throughout the Data Lifecycle. **(T-2)**

4.4.3. Data acquisition policies and processes must ensure compliance with standards and quality requirements. **(T-2)**

4.5. Data Storage, Integration, and Interoperability.

4.5.1. Data storage solutions (on-premise, cloud) must meet DoD security and compliance requirements (e.g., Impact Levels). **(T-2)**

4.5.2. Data integration processes must prioritize the use of standardized APIs and formats to ensure interoperability (aligning with AETC DAVE integration processes). **(T-2)**

4.5.3. Authoritative data sources must be accessible via registered APIs. **(T-2)**

4.5.4. Data architecture must facilitate management and integration, be documented, and align with enterprise architecture efforts interoperability. **(T-2)**

4.6. Data Mapping and System Integration Framework. To facilitate seamless data exchange, all student and learning information systems must adhere to standardized data mappings that ensure interoperability and consistency across platforms (see **Table 4.1.**). This framework establishes enterprise-wide compatibility and structured data governance, aligning with DoDI 1322.26 and DAFI 90-7001.

Table 4.1. Data Mapping and System Integration Framework.

Source System	Target System	Data Exchange Format	Purpose
LMS → LRS	Learning Record Store	xAPI	Track training records
LMS → SIS	Student Information System	API (JSON/XML)	Update official completion records
CBES → SIS	Student Information System	API (JSON/XML)	Track competency and certification history
HPMS → CBES	Competency-Based System	API (JSON)	Map physical performance data to competency tracking
TMS → LMS	Learning Management System	CSV/API	Import training event records

4.7. Scope, Applications, and Limitations. These integration standards define optimal configurations for systems operating within their designed scope and intended use; however, some units may adapt systems beyond their original specifications to fulfill mission-specific requirements. In such cases:

4.7.1. Documentation Requirement. Units implementing custom system configurations must document these modifications and their impact on standard integration patterns. **(T-3)**

4.7.2. Review and Modernization. Custom extensions, add-ons, or configurations preventing adherence to integration standards must be reviewed as part of system modernization planning. **(T-3)**

4.7.3. Operational Flexibility. These standards must be applied to the maximum extent possible without disrupting essential mission functions. **(T-3)**

4.7.4. This approach balances operational flexibility with the goal of achieving greater standardization and interoperability in future system iterations.

4.8. Integration Patterns and Best Practices. The following integration patterns represent best practices for ensuring system interoperability, efficient data exchange, and robust error handling across learning systems.

4.8.1. Real-Time vs. Batch Integration.

4.8.1.1. Real-time integration (via API) must be used for time-sensitive data exchanges, such as course completions and certification updates, to maintain accuracy and responsiveness. **(T-3)**

4.8.1.2. Batch integration (via scheduled file transfers) may be used for non-time-sensitive bulk data transfers, ensuring efficient handling of large datasets without overloading system resources.

4.8.1.3. Systems must document the integration pattern used for each type of data exchange to ensure transparency and consistency across implementations. **(T-3)**

4.8.1.4. **Example Applications:**

4.8.1.4.1. A LMS sends course completion and competency acquisition data to the SIS in real time via API to update student records immediately.

4.8.1.4.2. A training management system processes batch imports of historical training data from external sources during scheduled maintenance windows.

4.8.2. Error-Handling and Recovery.

4.8.2.1. All system integrations must implement structured error handling protocols to prevent disruptions. **(T-3)**

4.8.2.2. Failed data transfers must be logged and flagged for review to ensure a timely resolution. **(T-3)**

4.8.2.3. Systems must support automated retry mechanisms for failed transfers when appropriate, minimizing data loss. **(T-3)**

4.8.2.4. Critical integration failures must trigger real-time alerts to system administrators for immediate investigation and remediation. **(T-3)**

4.8.2.5. **Example Applications:**

4.8.2.5.1. If a competency-based system fails to synchronize certification records with the SIS, an error log is generated, and the system initiates an automatic retry.

4.8.2.5.2. A performance tracking system flags anomalous API failures and generates alerts for administrators to investigate potential security or connectivity issues.

4.8.3. Data Transformation and Normalization.

4.8.3.1. Systems using different data formats must implement transformation services to ensure compatibility across platforms. **(T-3)**

4.8.3.2. Field mapping documentation must be maintained for all integrations to facilitate seamless data interpretation and interoperability. **(T-3)**

4.8.3.3. Data normalization processes must ensure consistency across integrated systems, ensuring uniform representation of records. **(T-3)**

4.8.3.4. **Example Applications:**

4.8.3.4.1. A competency evaluation system transforms XML-based assessment data into JSON format before syncing with a central LRS.

4.8.3.4.2. An LMS normalizes training completion records by ensuring consistent formatting across multiple integrated platforms, reducing discrepancies in reporting.

4.9. Data Quality Management.

4.9.1. Data quality dimensions (e.g., accuracy, completeness, timeliness, consistency, relevance) must be defined, measured and monitored for critical data assets (aligning with AETC DAVE Quality Rules and Metrics) to ensure data is trusted and fit for purpose. **(T-2)**

4.9.2. Processes for data profiling, cleansing, validation, monitoring, and issue remediation must be established and implemented under the guidance of Data Stewards and Data Managers. **(T-2)**

4.9.3. The AETC Data Quality Standard must be followed to maintain the accuracy, completeness, consistency, and reliability of data assets. The Standard defines baseline requirements such as key data attributes, allowable formats, valid value ranges, validation checkpoints, and error resolution processes. Teams are responsible for creating detailed templates and specifications that align with these foundational requirements. **(T-2)**

4.10. Data Usage, Sharing, and Analytics.

4.10.1. Data must be made available to authorized users and systems through appropriate mechanisms, balancing access needs with security. **(T-2)**

4.10.2. Data sharing agreements must align with policy and guidance. **(T-2)**

4.10.3. Analytics efforts should leverage governed, high-quality data to generate Actionable Insights (AETC DAVE goal).

4.10.4. MDS's and data consumers must address ethical considerations and potential biases in data use, particularly for advanced analytics and AI/Machine Learning. **(T-2)**

4.11. Data Security and Privacy.

4.11.1. Data must be protected throughout its lifecycle according to its classification and sensitivity (e.g., Controlled Unclassified Information (CUI), PII, and Protected Health Information (PHI)). **(T-2)**

4.11.2. Security controls (e.g., access controls, encryption, authentication) must be implemented consistent with DoD and AF cybersecurity policies and aligned with AETC DAVE security policies to ensure comprehensive protection of sensitive information. **(T-2)**

4.11.3. Privacy requirements (e.g., AFI 33-332) must be strictly adhered to. **(T-2)**

4.12. Data Retention and Disposition.

4.12.1. Data will be retained and disposed of according to National Archives and Records Administration (NARA) General Records Schedule (GRS), Air Force Records Disposition Schedule (RDS), and AFI 33-322, as applicable. **(T-2)**

4.12.2. Data Stewards, in coordination with Records Management personnel, are responsible for ensuring retention schedules are applied to data assets within their domain.

4.12.3. Secure methods must be used for data disposal. **(T-2)**

4.13. Fostering a Data Culture.

4.13.1. AETC promotes a culture where data is valued, shared responsibly, and used ethically to inform actions and decisions at all levels (aligning with AETC DAVE Data Culture and Data Literacy initiatives).

4.13.2. Leadership must champion data-driven initiatives and empower the workforce through appropriate training and access to tools and data.

4.13.3. Collaboration across functional areas and stewardship roles is essential for maximizing the value derived from AETC's data assets.

4.14. Enabling Data-Informed Decisions.

4.14.1. The governance structure, standards, and processes outlined in this publication are designed to produce the high-quality, accessible, understandable, and trustworthy data required for reliable analytics and data-informed decision-making (AETC DAVE outcome: Efficient and Trusted Data-Informed Decisions).

4.14.2. Efforts must focus on linking data across domains to provide holistic insights supporting strategic planning, operational execution, and continuous improvement within the command.

4.15. Data Governance Maturity Model. Organizations must evaluate and enhance their data governance capabilities through a structured maturity model tailored to the military training environment (see **Table 4.2**.). Note: This Data Governance Maturity Model focuses specifically on data governance capabilities and processes. For evaluating the technical implementation and integration of learning systems, refer to the TLA Maturity Model described in **Chapter 5**, which provides guidance on assessing learning technology components and their interoperability, in accordance with DoDI 1322.26.

Table 4.2. Data Governance Maturity Levels.

Level	Criteria
Initial	Data governance is ad hoc with limited standardization and inconsistent practices.
Repeatable	Basic governance processes are defined, but their application is inconsistent across systems.
Defined	Standardized governance processes are implemented across most systems, fostering consistency.
Managed	Quantitative measures are used to evaluate data quality and governance effectiveness, enabling evidence-based improvements.
Optimizing	Governance processes are continuously refined and enhanced based on data-driven metrics and organizational feedback.

4.15.1. Organizations should periodically evaluate their data governance capabilities to identify strengths and improvement opportunities aligned with business objectives and available resources.

4.15.2. When governance gaps are identified, organizations must develop appropriate improvement strategies that balance maturity advancement with operational priorities. **(T-3)**

4.15.3. System acquisition and development planning must include an assessment of the organization's current data governance capabilities to identify additional governance resources needed, how the system will contribute to improved data governance maturity, and specific data governance requirements to include in system specifications and contracts. This approach ensures governance maturity is considered in acquisitions without creating artificial barriers for mission-critical systems. **(T-2)**

4.15.4. **Example Applications:**

4.15.4.1. A training command develops a structured plan to move from Level 2 (Repeatable) to Level 4 (Managed) governance maturity within 18 months by enhancing policy enforcement and monitoring mechanisms.

4.15.4.2. System modernization initiatives prioritize improvements in data governance capabilities, such as automated validation processes and robust metadata management.

4.16. Data Issue Resolution Framework. A structured and systematic approach to data issue resolution must be implemented to ensure timely identification, escalation, and remediation of data quality issues. (T-2)

4.16.1. Issue Identification and Classification.

4.16.1.1. Data quality issues must be categorized by severity, impact, and resolution complexity to prioritize remediation efforts effectively. **(T-3)**

4.16.1.2. Automated detection mechanisms must be integrated into workflows to proactively identify potential data issues and flag them for resolution. **(T-3)**

4.16.2. Escalation and Resolution.

4.16.2.1. Clearly defined escalation paths must be established to manage different types of data issues based on their criticality and scope. **(T-3)**

4.16.2.2. Service Level Agreements must be set to establish resolution timeframes and accountability for addressing issues promptly. **(T-3)**

4.16.2.3. Root cause analysis must be conducted for recurring issues to implement preventive measures and enhance system reliability. **(T-3)**

4.16.2.4. **Example Applications:**

4.16.2.4.1. Critical discrepancies in training certification data are resolved within 24 hours, ensuring minimal disruption to operational readiness.

4.16.2.4.2. A cross-functional team, including system owners and data stewards, collaborates to address complex data reconciliation challenges, reducing systemic risks.

Chapter 5

TOTAL LEARNING ARCHITECTURE MATURITY ASSESSMENT

5.1. TLA Maturity Model. The TLA Maturity Model provides a structured framework for organizations to evaluate and strategically plan their adoption of interoperable learning systems (see **Table 5.1**.). This model, aligned with DoDI 1322.26, defines five progressive levels of system integration and standards compliance, ensuring continuous advancement in digital learning capabilities.

Table 5.1. Total Learning Architecture Maturity Level.

Level	Criteria
1	Establishes foundational components including an LRS, LMS, and Analytics Dashboard to track learning activities.
2	Expands Level 1 capabilities by incorporating a Course Catalog, enabling structured access to training content.
3	Level 2 components plus Enterprise Course Catalog (ECC) Competency Registry and Experience Index.
4	Level 3 components with full integration of the ECC Competency Registry and Experience Index.
5	Level 4 components plus Learner Profile, Enterprise Learner Record Repository (ELRR), and integration with Manpower and Personnel Systems.

5.2. Standards Compliance Scoring. Each system component is scored on a 1-5 scale for standards compliance implementation. This approach provides a quantifiable metric for assessing system maturity and alignment with TLA interoperability objectives, supporting long-term integration efforts.

5.2.1. xAPI Structuring and Processing: Evaluates the proper formatting, tracking, and integration of learning experience data using xAPI.

5.2.2. cmi5 Structuring and Processing: Assesses system support for the cmi5 standard, ensuring accurate course package interoperability.

5.2.3. P2881 Learning Metadata Terms Structuring: Measures adherence to Institute of Electrical and Electronics Engineers (IEEE) P2881 metadata standards for consistent learning object descriptions.

5.2.4. Sharable Competency Definitions (SCD) Structuring: Determines compliance with structured competency definitions, enabling standardized skill tracking.

5.2.5. Enterprise Learner Record (ELR) Structuring: Verifies proper implementation of ELR frameworks to ensure centralized learner progress tracking and data portability.

5.3. Implementation Considerations. Mission Data Stewards must evaluate their current TLA Maturity Level as part of system planning to guide future improvements in learning system integration. **(T-3) Note:** The TLA Maturity Model focuses specifically on the technical implementation and integration of learning systems. For evaluating organizational data governance capabilities, refer to the Data Governance Maturity Model in **paragraph 4.15** which provides a framework for data quality management, stewardship, and governance processes.

5.3.1. Strategic Advancement: New system acquisitions should align with efforts to progress toward the next appropriate maturity level, ensuring continuous enhancement.

5.3.2. Data Integration Assessment: The interoperability and data exchange between system components must be evaluated as part of the maturity assessment to identify potential gaps and optimization opportunities. **(T-3)**

5.3.3. Roadmap Development: Organizations must establish a structured roadmap for advancing through the maturity levels over time, ensuring a phased and strategic approach to system evolution. **(T-3)**

Chapter 6

DATA PRIVACY AND SECURITY

6.1. Data Privacy and Security Standards. This section establishes data privacy and security standards for AETC information systems that handle student and learning data within the military training and development context. Establishing robust privacy and security practices is critical for:

6.1.1. Protecting PII and sensitive data from unauthorized access or misuse.

6.1.2. Ensuring compliance with DoD and AF data security policies and records management directives to maintain regulatory accountability.

6.1.3. Maintaining secure system integrations and controlled data sharing to safeguard the integrity of interconnected systems.

6.1.4. Preventing data breaches and unauthorized access ensuring uninterrupted operation and data security.

6.2. Policy. This section aligns with the policies and directives listed in **Table 3.1** to ensure systems handling training, education, and personnel-related data comply with DoD/AF standards.

6.3. Data Privacy Requirements. All information systems must implement structured data privacy controls to safeguard PII, training records, competency data, and performance assessments, ensuring compliance with DoD standards. **(T-2)**

6.3.1. Data Classification and Protection.

6.3.1.1. All data must be classified appropriately based on DoD sensitivity levels (e.g., CUI). **(T-2)**

6.3.1.2. PII and training records must be encrypted at rest and in transit to prevent unauthorized access or breaches. **(T-2)**

6.3.1.3. Privileged users must enforce role-based access controls (RBAC) to restrict data access based on user roles and clearance levels. **(T-2)**

6.3.1.4. **Example Application:** A system tracking military certifications and qualifications must ensure that rank, DoD ID, and competency data are stored securely and inaccessible to unauthorized users.

6.3.2. Access Control and Authentication.

6.3.2.1. All information systems processing, storing or transmitting training or personnel data must require DoD Approved MFA for access. **(T-2)**

6.3.2.2. The principle of least privilege must be enforced, allowing users to access only the data necessary to perform their duties. **(T-2)**

6.3.2.3. System logs must track and audit all data access events to identify anomalies and prevent insider threats. **(T-2)**

6.3.2.4. **Example Applications:**

6.3.2.4.1. An instructor managing student enrollments in a training platform is restricted from editing personnel records beyond their assigned role to maintain system integrity.

6.3.2.4.2. A database storing biometric performance data logs all access attempts and flags unauthorized login attempts for immediate review.

6.3.2.5. ICAM Requirements: To meet Identity, Credentialing, and Access Management (ICAM) standards, systems must comply with DAFMAN 17-1304, *Identify, Credential and Access Management (ICAM)* which covers:

6.3.2.5.1. CAC/PIV authentication, and handling of DoD ID numbers in xAPI statements. **(T-2)**

6.3.2.5.2. Integration of ICAM integration with learning systems to ensure secure and centralized access control. **(T-2)**

6.3.3. Data Retention and Disposal.

6.3.3.1. All records must be maintained and disposed of in accordance with AFI 33-322 and the Air Force RDS.

6.3.3.2. Training records and competency assessments must be archived securely before disposal. **(T-3)**

6.3.3.3. Automated deletion processes should be implemented to remove outdated or obsolete records while ensuring compliance with retention policies.

6.3.3.4. **Example Applications:**

6.3.3.4.1. A training management system should automatically remove outdated competency assessments after five years unless flagged for retention

6.3.3.4.2. A system used for tracking mission readiness data must store records in compliance with Air Force RDS before secure disposal.

6.3.4. Incident Response and Data Breach Protocols.

6.3.4.1. All systems must have a documented incident response plan outlining steps to address potential data breaches and mitigate risks. **(T-2)**

6.3.4.2. Any instance of unauthorized access, data loss, or data breach must be reported immediately to the Information Assurance team per DoD policies. **(T-2)**

6.3.4.3. Automated alerting mechanisms must be implemented to detect and respond to suspicious activities such as unauthorized login attempts or anomalous data requests. **(T-3)**

6.3.4.4. **Example Application:** A system triggers an alert and temporarily restricts access if a user attempts to download an unusually large volume of personnel records outside normal business hours. A student performance tracking system must flag and log unauthorized API requests for data extraction, enabling swift investigation and resolution.

6.4. Data Security Requirements for System Integrations. All system integrations must adhere to strict security protocols to prevent unauthorized data access, data leakage, and ensure the integrity of shared information.

6.4.1. Secure API Integration.

6.4.1.1. APIs facilitating data exchange must be secured using industry-standard methods, including OAuth 2.0, Public Key Infrastructure certificates, or mutual transport layer security (TLS) to ensure authentication and data protection. **(T-2)**

6.4.1.2. All data in transit must be encrypted using *Federal Information Processing Standard* 140-3 approved TLS, version 1.2 or higher, to prevent interception or compromise during transmission. **(T-2)**

6.4.1.3. Integration logs must track all API transactions to maintain data integrity and provide an audit trail for detecting unauthorized access or anomalies. **(T-3)**

6.4.1.4. **Example Applications:**

6.4.1.4.1. A competency-based system exchanging training completion data with a central records management tool must ensure all API requests are encrypted and authenticated.

6.4.1.4.2. A biometric data tracking system must validate all outbound data transmissions before sending information to another database, ensuring compliance with security standards.

6.4.2. Role-Based Access for Data Sharing.

6.4.2.1. Role-based permissions must be enforced across all integrated systems to limit user access, ensuring only authorized personnel can access, edit, or transfer sensitive data. **(T-2)**

6.4.2.2. Integration points must adhere to defined access control policies to restrict excessive or unnecessary data exposure. **(T-2)**

6.4.2.3. **Example Applications:**

6.4.2.3.1. A learning system explicitly restricts student PII from being shared with external reporting tools unless specifically authorized. A mission training platform enforces access controls to prevent unauthorized third-party vendors from retrieving competency evaluation data.

6.4.2.3.2. Student and learning data may require tailored security controls based on its sensitivity level and use case to ensure proper protection and compliance.

6.4.3. Biometric and Performance Data Security.

6.4.3.1. Biometric data collected by human performance management systems must be classified in accordance with DOD Manual 6025.18, *Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs,* due to its personal and potentially critical nature. **(T-0)**

6.4.3.2. Systems capturing physiological measurements must implement enhanced anonymization measures when sharing this data across platforms to prevent misuse. **(T-2)**

6.4.3.3. Access to biometric data must be strictly limited and require additional layers of authorization to minimize risks. **(T-2)**

6.4.3.4. **Example Applications:**

6.4.3.4.1. A learning system labels applicable biometric data containing PHI correctly in the system of record.

6.4.3.4.2. A learning system uses enhanced anonymization measures to transmit biometric PHI data.

6.4.4. XR Data Security.

6.4.4.1. XR systems that capture user movements, interactions, and performance metrics must implement security controls tailored to the sensitivity of this data to safeguard user privacy and system integrity. **(T-2)**

6.4.4.2. For standalone XR systems, local data must be encrypted and secured against unauthorized access to prevent data breaches. **(T-2)**

6.4.4.3. Data transfer procedures for standalone XR systems must include comprehensive security validation steps to ensure the integrity and protection of data before integration with enterprise systems. **(T-2)**

6.4.4.4. **Example Applications:**

6.4.4.4.1. Encryption safeguards user interaction data stored locally in standalone XR training systems.

6.4.4.4.2. Data transfers from standalone XR platforms are validated for compliance with organizational security protocols before synchronization with enterprise databases.

6.4.5. Competency and Certification Data.

6.4.5.1. Systems managing competency and certification records that impact career progression must implement heightened security measures to ensure data integrity and trustworthiness. **(T-2)**

6.4.5.2. Digital credential verification systems must include anti-tampering mechanisms to prevent falsification or unauthorized modifications. **(T-2)**

6.4.5.3. Access controls for certification modification functions must be strictly enforced and include regular audit trails to ensure accountability and compliance. **(T-2)**

6.4.5.4. **Example Applications:**

6.4.5.4.1. Credentialing systems use anti-tampering safeguards to verify the authenticity of certifications issued to personnel.

6.4.5.4.2. Audit logs track and record all modifications made to certification data, ensuring transparency and mitigating risks of unauthorized changes.

6.4.6. Data Sanitization for Cross-Domain Transfers.

6.4.6.1. Data moving across security domains must undergo appropriate sanitization processes to ensure classified or sensitive information is removed or appropriately masked. **(T-2)**

6.4.6.2. Automated content validation tools must be implemented to check and confirm the data’s security compliance before cross-domain transfer. **(T-2)**

6.4.6.3. **Example Applications:**

6.4.6.3.1. Performance data from a classified training environment must be sanitized to remove sensitive mission details before transferring to an unclassified student record system.

6.4.6.3.2. Cross-domain guards must be configured to block unauthorized data types from crossing security boundaries, mitigating the risk of classified information leakage.

6.5. Supply Chain Security. System owners must implement comprehensive controls to address security risks associated with the software and hardware supply chain to ensure data protection and operational integrity. (T-2)

6.6. Security Training Requirements. All personnel responsible for administering or using student and learning information systems must receive appropriate security training to ensure the protection of sensitive data and compliance with DoD standards.

6.6.1. Administrator Training. Database administrators responsible for managing student records must receive in-depth training on data protection requirements to safeguard sensitive information.

6.6.1.1. System administrators must complete specialized security training appropriate to their roles and responsibilities. **(T-2)**

6.6.1.2. Training must be refreshed annually and whenever significant system changes occur to ensure administrators stay updated on current practices. **(T-3)**

6.6.1.3. Administrators must demonstrate competency in security procedures before being granted elevated system access. **(T-3)**

6.6.1.4. **Example Application:** LMS administrators must complete training on secure configuration practices before being granted system access.

6.6.2. End User Security Training.

6.6.2.1. Users with access to sensitive data must receive additional role-specific security training to address the unique risks associated with their responsibilities. **(T-2)**

6.6.2.2. Training completion must be tracked and verified before granting users access to the systems. **(T-3)**

6.6.2.3. **Example Applications:**

6.6.2.3.1. Instructors with access to student performance data must complete privacy training to ensure compliance before being granted system access.

6.6.2.3.2. Users must demonstrate understanding of phishing prevention techniques and other cybersecurity best practices before accessing systems containing sensitive data.

CLARK J. QUINN, Maj Gen, USAF
Deputy Commander, Air Education and Training Command

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 17-130, *Cybersecurity Program Management*, 12 February 2020

AFI 33-322, *Records Management and Information Governance Program*, 23 March 2020

AFI 33-332, *Air Force Privacy and Civil Liberties Program*, 10 March 2020

AFPD 90-70, *Enterprise Data Management*, 13 February 2020

DAFI 90-160, *Publications and Forms Management*, 14 April 2022

DAFI 90-7001, *Enterprise Data Sharing and Data Stewardship*, 22 April 2021

DAFMAN 17-1304, *Identify, Credential and Access Management (ICAM)*, 17 August 2021

DAFMAN 90-161, *Publishing Process and Procedures*, 15 April 2022

DoD Data Stewardship Guidebook, October 2021

DoDI 1322.26, *Distributed Learning*, 05 October 2017

DoDI 8510.01, *Risk Management Framework for DoD Systems*, 19 July 2022

DoDM 6025.18, *Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs*, 13 Mar 2019

OneRoster (IMS Global Standard), Spec Version 1.2, 19 September 2022

Total Learning Architecture Standards Digital Learning Acquisition Techniques, December 2023

Prescribed Forms

None

Adopted Forms

DAF Form 847, *Recommendation for Change of Product*

Abbreviations and Acronyms

AETC—Air Education and Training Command

AF—Air Force

AFI—Air Force Instruction

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

ANG—Air National Guard

API—Application Programming Interface

AR—Augmented Reality

C&IT—Cyberspace and Information Technology

CBES—Competency-Based Education Systems

CDO—Command Data Officer

CIO—Chief Information Officer

CLO—Chief Learning Officer

CMI5—Computer-Managed Instruction

COMAETC—AETC Commander

CSV—Comma-Separated Values

CTO—Chief Technology Officer

CUI—Controlled Unclassified Information

DAF—Department of the Air Force

DAFI—Department of the Air Force Instruction

DAFLR—DAF Learning Record

DAFMAN—Department of the Air Force Manual

DAVE—Data and Analysis Virtual Ecosystem

DCOM—AETC Deputy Commander

DCWG—Data Connections Working Group

DGWG—Data Governance Working Group

DoD—Department of Defense

DoDI—Department of Defense Instruction

DoDM—Department of Defense Manual

EAWG—Enterprise Architecture Working Group

ECC—Enterprise Course Catalog

EDM—Enterprise Data Management

ELR—Enterprise Learner Record

ELRR—Enterprise Learner Record Repository

ETL—Extract, Transform, Load

GRS—General Records Schedule

HPMS—Human Performance Management Systems

ICAM—Identity, Credentialing, and Access Management

IDOG—IT Data Oversight and Governance

IS—Information Systems

ISO—International Organization for Standardization

IT—Information Technology

JSON—JavaScript Object Notation

LMS—Learning Management System

LRS—Learning Record Store

LTI—Learning Tools Interoperability

MDS—Mission Data Steward

MFA—Multi-Factor Authentication

MOA—Memorandum of Agreement

MOU—Memorandum of Understanding

NARA—National Archives and Records Administration

OPR—Office of Primary Responsibility

PHI—Protected Health Information

PII—Personally Identifiable Information

RBAC—Role-Based Access Controls

RDS—Records Disposition Schedule

SCORM—Sharable Content Object Reference Model

SDM—Service Data Manager

SIS—Student Information System

TAA—Training Affiliation Agreement

TDC—Technical Data Custodian

TDSG—Technical Data Standards Guide

TLA—Total Learning Architecture

TLS—Transport Layer Security

TMS—Training Management Systems

TOPS—Technical and Operational Practices and Standards

TTMS—Tech Training Management System

USSF—United States Space Force

VAULTIS—Visible, Accessible, Understandable, Linked, Trustworthy, Interoperable, Secure

VR—Virtual Reality

xAPI—Experience Application Programming Interface

XML—Extensible Markup Language

XR—Extended Reality

Office Symbols

SAF/CO—Air Force Chief Data Officer

SAF/FM—Assistant Secretary of the Air Force for Financial Management and Comptroller

AF/A1—Air Force Deputy Chief of Staff, Manpower and Personnel

AETC/A3/6—Directorate of Operations and Communications

Terms

Application Programming Interface—A set of rules that allows software systems to communicate, enabling secure and automated data exchange between applications.

Augmented Reality/Virtual Reality Systems—Immersive training environments simulating real-world scenarios via VR headsets, AR overlays, and 3D training modules. These systems must support xAPI for tracking learner progress, be network-compatible and avoid standalone deployment, and integrate with existing learning ecosystems as specified in DoDI 1322.26. **Examples:** Tactical VR Simulators and AR Training Modules.

Competency—Based Education System—A platform for tracking competency attainment, skill development, and certifications across a learner's career. These systems must integrate competency frameworks with LMS, TMS, and HPMS; support automated skill tracking and credential validation; and align with DAFPD 36-26. **Examples:** Workday Skills Cloud, Degreed, and Cornerstone.

Data—Recorded information, regardless of form or the media on which it is recorded (44 USC § 350)**.**

Data Governance—The exercise of authority, control, and shared decision making (planning, monitoring, and enforcement) over the management of data assets. (DAMA DMBOK 2nd Edition)

Data Integration—The process of combining data from different sources to provide a unified view for users while maintaining accuracy and context.

Data Lineage—Documentation of where data originates, how it moves through systems, and how it transforms throughout its lifecycle.

Data Standard—A documented agreement and specification by an authoritative body on a definition, representation, or format of data, metadata, or exchange protocol that is used to improve data understanding and data interoperability. A data standard requires a narrative specification and may include complementary data engineering resources to guide IT system development and testing conformance. Widespread adoption of a well-designed data standard can reduce ambiguity and the necessity for mediation, while promoting efficiency and transparency of mediation where required (DoDI 8320.07)

Data Steward—Data stewards manage data assets on behalf of others and in the best interest of the organization. Data stewards represent the interest of all stakeholders and must take an enterprise perspective to ensure enterprise data is of high quality and can be used effectively. Based on the stewardship framework, data stewards are differentiated by their place within the organization and by the focus of their work. (DAMA DMBOK 2nd edition)

Data Stewardship—The formal accountability for management of data assets to ensure fitness for use, security, and compliance with policy.

Enterprise Data Management—Development and execution of plans, policies, programs and practices (4Ps) that acquire, control, protect and enhance the value of data assets throughout the lifecycle, led or performed by data professionals following established disciplines and functions. (DoD Office of the Chief Information Officer Memorandum, *DoD Data Management Lexicon*, dated June 15, 2020, as derived from DAMA DMBOK 2nd Edition, 2017. IC Chief Data Officer Council (CDOC) Approved: Jun 2018).

Experience Application Programming—Interface (formerly Tin Can API)—A data standard for tracking learning experiences across multiple platforms, allowing organizations to capture, store, and analyze learning activities beyond traditional LMS environments.

Extended Reality—An overarching concept encompassing augmented reality (AR), virtual reality (VR), mixed reality (MR), haptic technology, and other existing and future technologies that create and present digital audio, visual, or tactile representations of the physical world to a user, commonly via a handheld or wearable computing device.

Guidance—Statement of important, high-level direction that guides decisions and actions throughout the DAF. Guidance translates the ideas, goals, or principles contained in the mission, vision, and strategic plan into actionable directives. (See DAFI 90-160 and DAFMAN 90-161 for details).

Human Performance Management System—A system used for monitoring and analyzing personnel's physical, cognitive, and mental performance metrics. These systems must support biometric data security and DoD privacy guidelines, enable data sharing with TMS and CBES for competency tracking, and protect sensitive medical and performance data per AFI 33-332. Examples: Smartabase, Military Operational Performance and Physical Status System (MOPPPS), and other military performance monitoring platforms.

Interoperability—The ability of systems, units, or forces to provide data, information, materiel, and services to, and accept the same from, other systems, units or forces, and to use the data, information, materiel, and services exchanged to enable them to operate effectively together. IT interoperability includes both the technical exchange of information and the end-to-end operational effectiveness of that exchange of information as required for mission accomplishment. Interoperability is more than just information exchange. It includes systems, processes, procedures, organizations, and missions over the life cycle and must be balanced with cybersecurity (DoDI 8330.01).

Learning Management System—Software application dedicated to the delivery of educational content, training programs, and the management of learning data. It facilitates the administration, documentation, tracking, reporting, and delivery of educational courses and learning activities, capturing and storing data related to learner engagement, progress, and outcomes such as grades and assessments. An LMS provides interactive features such as threaded discussions, video conferencing, discussion forums, and may incorporate AI tools, like chatbots, to support the learning process. While an LMS may interface with an SIS, it is a separate application focused on content delivery and learner engagement. LMS applications may require customization before deployment or during their lifecycle to meet the Air Force or military's specific operational requirements, security protocols, and network specifications. These systems must support

SCORM/xAPI for course content tracking, enable API-based integration with SIS, and may require customization before deployment to meet DoD security requirements. **Examples:** Blackboard, Moodle, Canvas, and DoD-specific LMS platforms.

Learning Record Store—A system for capturing, storing, retrieving, and analyzing xAPI-based learning activity data. An LRS includes both backend database functionality for storing xAPI statements and a user interface for administrators and analysts to query data, create visualizations, generate reports, and manage integrations with other learning systems. These systems must ingest xAPI statements from LMS, XR platforms, and competency-based assessments; provide reporting dashboards for training effectiveness analysis; support data retention policies per AFI 33-322; and enable integration with other learning systems to create a comprehensive view of learning activities. **Examples:** Learning Locker, Watershed LRS, Yet Analytics, and Veracity LRS.

Learning Tools Interoperability—A standard that enables third-party learning tools to be integrated into an LMS with minimal configuration, ensuring seamless interaction.

Other Student and Learning Data Systems—Any additional information system that collects, processes, stores, or transmits student or learning data, regardless of its primary function. These systems must comply with basic interoperability standards, enable data extraction and migration, document data structures and integration points, and support secure authentication methods consistent with DoD requirements. **Examples:** Content Management Systems (CMS) used for educational material, Assessment platforms, Digital credentialing systems, Mobile learning applications, Collaborative learning tools, Career development systems, Intelligent tutoring systems, and Course scheduling applications.

Metadata—Structural or descriptive information about data such as content, format, source, rights, accuracy, provenance, frequency, periodicity, granularity, publisher or responsible party, contact information, method of collection, and other descriptions (44 USC § 3502).

Metadata Management—The administration of data that describes other data, focusing on defining and maintaining consistent definitions, relationships, and provenance.

Sharable Content Object Reference Model—A widely used standard for structuring and delivering e-learning content in LMS platforms, ensuring consistent course packaging and tracking.

Student Information System—Software application that manages and stores comprehensive student-related data, supporting administrative and academic processes within an organization. An SIS provides capabilities including student registration, scheduling, documenting grades, transcripts, assessment scores, tracking attendance, and managing other student-related data needs. While an SIS may interface with other applications like a LMS, it is a distinct system focused on tracking and managing student information. SIS applications may require customization before deployment or during their lifecycle to meet the Air Force or military's specific operational requirements, security protocols, and network specifications. These systems must allow structured data exports for training reports, enable secure integration with LMS and CBES to track learning progression, and comply with DoD privacy requirements for Personally Identifiable Information. **Examples:** Oracle PeopleSoft, PowerSchool, and DoD Military Education Systems.

Records Management—The systematic control of records from creation or receipt through processing, distribution, organization, and retrieval to disposition.

System Integration—The process of linking multiple IT systems to enable automated data sharing and improve operational efficiency.

Standalone Application—A software system that operates independently, lacking built-in integration capabilities, often requiring manual data transfer.

Training—Formal and informal learning focused on proficiency development, which is the attainment and retention of skills, knowledge, and attitudes required to meet specific function or job performance requirements.

Training Management System—A system used for scheduling, tracking, and managing hands-on and operational training events. These systems must enable automated tracking of certifications and training events, support real-time data reporting for leadership decision-making, and align with operational training requirements. **Examples:** Graduate Training Integration Management System (GTIMS) and DoD Tactical Training Systems.

Attachment 2

COMMON DATA ELEMENTS

A2.1. Overview. Paragraph A2.2. provides both functional descriptions of data elements and **paragraph A2.3** provides their technical implementation requirements. Together, these paragraphs establish a complete understanding of each data element for both business and technical stakeholders. The data elements defined in this attachment are referenced throughout the main document and establish standard definitions to ensure consistent implementation across AETC information systems.

A2.2. Data Element Descriptions.

A2.2.1. Student ID. A unique identifier assigned to each learner to ensure accurate tracking of their training records, progress, and credentials across systems.

A2.2.2. Rank. Refers to the military rank of the learner, providing context for training requirements, eligibility, and role-based learning paths.

A2.2.3. Organization. Indicates the unit, department, or command to which the learner is assigned, supporting reporting, access control, and organizational readiness assessments.

A2.2.4. Training Course ID. A unique identifier assigned to each course, allowing systems to distinguish between different training offerings and ensuring consistency in tracking course enrollments and completions.

A2.2.5. Competency ID. An identifier for a defined competency or skill that a learner is expected to develop or demonstrate, enabling alignment with performance frameworks and career progression.

A2.2.6. Completion Status. Tracks whether a learner has completed a specific course or demonstrated a required competency, providing visibility into individual and organizational learning outcomes.

A2.2.7. Training Hours Logged. Reflects the total number of hours a learner has spent engaging with training modules, supporting compliance tracking, performance evaluation, and time allocation metrics.

A2.2.8. XR Session Data. Captures detailed user interactions, behavioral patterns, and performance metrics within augmented or virtual reality training environments, allowing for in-depth analysis of experiential learning.

A2.2.9. Certification Expiration Date. Tracks when a learner's certification or demonstrated competency must expire, enabling timely recertification and ensuring continued operational readiness.

A2.2.10. Assessment Score. A numerical or categorical evaluation of learner performance on a given assessment, used to measure knowledge retention, skill proficiency, and progress toward training objectives.

A2.2.11. Instructor ID. An identifier assigned to the individual responsible for delivering or evaluating the training, enabling traceability, quality control, and reporting on instructional activities.

A2.2.12. Course Version. An identifier that distinguishes a specific iteration or release of training content, ensuring learners are engaging with the most current material and allowing historical tracking of changes over time.

A2.2.13. Learning Objective ID. An identifier for a specific educational goal or outcome within a training program, supporting alignment between instructional content, assessments, and desired competencies.

A2.3. Data Technical Implementation Requirements. Table A2.1 provides the technical specifications required for implementing the data elements described in **paragraph A2.2**. These specifications ensure consistency and interoperability across all AETC information systems that handle student and learning data.

Table A2.1. Detailed Data Element Specifications.

Data Element	Data Type	Format	Constraints	Implementation Notes
Student ID	String	Alphanumeric, 10 chars	Must match DoD ID format	Primary key for student records; must be used as foreign key in all related tables
Rank	String	Per AETC Metadata Standard v1.0	Must use standardized military rank codes	Must support both displayed values (e.g., "TSgt") and stored values (e.g., "E-6")
Organization	String	Per AETC Metadata Standard v1.0	Must follow official organizational hierarchy	Must maintain parent-child relationships in organizational hierarchy
Training Course ID	String	Alphanumeric, 8-12 chars	Must be unique across all systems	Must follow standardized course numbering system defined in AETC Metadata Standard v1.0
Competency ID	String	Alphanumeric prefix + numeric ID	Must be unique and traceable	Must map to authoritative competency framework
Completion Status	Enumeration	Text or numeric code	Limited to approved status values	Must support standard status progression and history tracking
Training Hours	Numeric	Decimal (##.#)	Non-negative value	Must support cumulative and

Logged				individual session tracking
XR Session Data	JSON	xAPI statement format	Must include all required xAPI fields	Must capture user interactions and performance within immersive training environments
Certification Expiration Date	Date	ISO 8601 (YYYY-MM-DD)	Valid date, not in past	Must include time zone information for global operations
Assessment Score	Numeric	Decimal (###.##)	Range: 0-100 or system-specific	Must support both raw scores and calculated percentages
Instructor ID	String	Alphanumeric, 10 chars	Must match DoD ID format	Must link to personnel table with instructor qualifications
Course Version	String	SemVer format (x.y.z)	Must follow version control standards	Must track content revisions and maintain backward compatibility
Learning Objective ID	String	Alphanumeric	Must be unique within course	Must map to authoritative learning taxonomy