**XII. Appendix G**

**Technical Requirements Part I Functional Requirements**

**Instructions: The Resource submitted shall support vertical alignment for Mathematics Course Beyond Algebra II. The Offeror must provide at least one example to show how the proposed Resource meets or exceeds the Mandatory or Desired requirements below**. The Offeror should include screenshots, excerpts, or images from the Resource to illustrate or explain each example rather than simply referencing certain page numbers in a teacher edition.

**~~VDOE Mathematics Standards of Learning can be found here:~~** [**~~https://www.doe.virginia.gov/testing/sol/standards\_docs/mathemati~~**](http://www.doe.virginia.gov/testing/sol/standards_docs/mathematics/index.shtml)**~~cs/i~~**[**~~ndex.shtml~~**](http://www.doe.virginia.gov/testing/sol/standards_docs/mathematics/index.shtml)

VDOE Mathematics Standards of Learning can be found here:

[https://www.doe.virginia.gov/teaching-learning-assessment/instruction/mathematics/standards-of-learning-for-mathematics](http://www.doe.virginia.gov/teaching-learning-assessment/instruction/mathematics/standards-of-learning-for-mathematics)

*\*Algebra III course should align with the VDOE mathematics standards for Trigonometry.*

*\*Pre-Calculus course should align with the VDOE mathematics standards for Mathematical Analysis and Trigonometry.*

*\*All AP courses should be aligned with College Board Course Descriptions/Framework*

**~~Math Process Goals can in the~~ *~~Introduction~~* ~~section of the following document:~~** [**~~https://www.doe.virginia.gov/testing/sol/standards\_docs/mathematics/2016/cf/mathanal~~**](http://www.doe.virginia.gov/testing/sol/standards_docs/mathematics/2016/cf/mathanalysis-cf.pdf)**~~ysis-c~~**[**~~f.pdf~~**](http://www.doe.virginia.gov/testing/sol/standards_docs/mathematics/2016/cf/mathanalysis-cf.pdf)

Math Process Goals are in the Introduction section of the following document, page 2: [https://www.doe.virginia.gov/home/showpublisheddocument/3046/637982465193330000](http://www.doe.virginia.gov/home/showpublisheddocument/3046/637982465193330000)

|  |  |  |
| --- | --- | --- |
| **Section a. Mathematics Resources**  . | **Mandatory or Desired** | **Yes or No** |
| Aligns with the 2016 Virginia Standards of Learning for Mathematics (non-AP courses)\*. | Mandatory |  |
| Aligns with the 2016 Virginia Mathematics Process Goal; Mathematical Problem Solving\*. | Mandatory |  |
| Aligns with the 2016 Virginia Mathematics Process Goal; Mathematical Communication\*. | Mandatory |  |

55

Appendix G– Technical Requirements Part I

|  |  |  |
| --- | --- | --- |
| Aligns with the 2016 Virginia Mathematics Process Goal; Mathematical Reasoning\*. | Mandatory |  |
| Aligns with the 2016 Virginia Mathematics Process Goal; Mathematical Connections\*. | Mandatory |  |
| Aligns with the 2016 Virginia Mathematics Process Goal; Mathematical Representations\*. | Mandatory |  |
| Has flexible sequencing – provide examples within the materials that shows curriculum can be integrated | Mandatory |  |
| Has online tools for teacher use | Mandatory |  |
| Has online tools for student use | Mandatory |  |
| Provides a bank of number sense routines | Desired |  |
| Variety of rich activities, tasks, and simulations (statistics courses) beyond traditional problem sets | Mandatory |  |
| AP Exam aligned assessment practice (AP courses) | Mandatory |  |
| Supports for English Learners – language acquisition/vocabulary | Mandatory |  |
| Digital materials available in Spanish | Desired |  |

|  |  |  |
| --- | --- | --- |
| **Section b. Assessments – Summative and Formative** | **Mandatory or Desired** | **Yes or No** |
| Include formative assessments, including pre-assessments, to determine student understanding | Mandatory |  |
| The resource provides guidance and a bank of lessons and/or activities based on assessment results | Desired |  |
| The resource may include summative assessments to determine student progress *(AP course assessment structure mirrors AP exam)* | Desired |  |
| The resource may include progress monitoring measures. | Desired |  |

56

Appendix G– Technical Requirements Part I

|  |  |  |
| --- | --- | --- |
| **Section c. Professional Learning and Coaching** | **Mandatory or Desired** | **Yes or No** |
| The Offeror can provide professional learning both in person and virtual options for implementation of the product. | Mandatory |  |
| The Offeror can provide professional learning and coaching on the resources in July and August 2023, for up to 30 teachers per professional learning and coaching course, with multiple professional learning and coaching courses offered. | Mandatory |  |
| The Offeror can provide on-going professional learning and coaching on the resources throughout the school-year and throughout the life of the contract. | Mandatory |  |

Appendix G– Technical Requirements Part I 57

**XII. Appendix G** **Technical Requirements, Part II**

**APS Information Technology Service Management Quality Assessment**

The following tables are the basis for the technological quality assessment of the offering. The responses, information, and documentation provided will allow APS to assess the underlying quality of the technology offering. This is not an assessment of the features, functionality, or quality of the offering for its intended use or purpose, but an assessment of the quality and capabilities of the underlying technology, the development and support structures that allow the offering to function, and the compatibility of these technical elements with the existing technological infrastructure utilized and maintained by Arlington Public Schools.

The responses, information, and documentation provided should allow APS to make initial assessments of the effort involved to integrate and maintain the offering with our existing technology infrastructure as well as make some preliminary assessment of the cybersecurity risks involved with adoption of the offering.

Both the quality and capabilities of the underlying technology and its development and support structures, as well as the effort involved to integrate and maintain the offering, represent cost and value in APS time and resources over the lifetime use of the offering. In order to minimize costs and maximize value, APS will use this qualitative assessment as part of the overall evaluation of the offering.

In order to allow for detailed and complete responses to this assessment, each element is indexed with an “APS Reference” label. Any auxiliary documentation supplied should be labeled with the appropriate “APS Reference” label so that all parts of the response can be properly attributed to the correct assessment element.

Not all elements will apply to all offerings; Leaving an element blank (no response) is a valid response, but comprehensive responses are preferred where applicable.

HTTP references to **publicly available** online documentation are acceptable; specific location (page, section paragraph, etc.) should be specified in order to expedite review.

Non-Disclosure Agreements (NDAs) that cover proprietary vendor technical information may be allowed to facilitate effective disclosure.

**( 2022-05-27a )**

**APS Information Technology Environment**

**Notes:**

The following table provides information on the technology environment and basic expectations maintained by Arlington Public Schools. The offering should be responsive to this environment and the noted expectations. The Offeror should provide inline or referenced documentation on how their offering would integrate with, and function within this environment. Please note any deviation of claimed functionality between platforms or limitations of some platforms vs others. Not all offerings will interact with all platforms; "Not Applicable" is a valid response.

Please provide inline responses in the lower sections marked with “ ⌇ “ or provide indexed auxiliary responses, notes, comments, or documentation using the "*APS Reference*" field as the cross-reference key.

|  |  |  |
| --- | --- | --- |
| **APS Reference** | **Description** | **Notes** |
|  |  |  |
|  | **Client Platforms** | |
| **iOS** | **Apple iPads**  **(approx. ~25,000)** | **APS provides all Elementary (K-5) and Middle (6-8) school students with individual personally assigned Apple iPads that are managed via MDM.**  **APS also may provide MDM managed Apple iPads to some classroom and administrative staff** |
| **iOS** | ⌇ | |
| **iOS-App** | Vendor provides an iOS **Application**, deployed via the Apple App Store | Offeror should document the capacities and limitations of the vendor supported iOS Apps relevant to the offering. |
| **iOS-App** | ⌇ | |
| **iOS-Web** | Vendor provides a browser based service that is functional using Apple **Safari** under iOS on an Apple iPad device. | Offeror should document the capacities and limitations of the vendor supported web service relevant to the offering, when accessed via the Apple Safari browser on an Apple iPad device. |
| **iOS-Web** | ⌇ | |
| **MacOS** | **Apple MacBooks**  **(approx. ~12,000)** | **APS provides all High School (9-12) students with individual personally assigned Apple MacBooks that are managed via MDM.**  **APS also may provide MDM managed Apple MacBooks to classroom teachers and administrative staff** |
| **MacOS** | ⌇ | |
| **MacOS-App** | Vendor provides a native MacOS Application, deployed via the **Apple App Store** | Offeror should document the capacities and limitations of the vendor supported MacOS Application relevant to the offering. Document any dependencies or requirements the software may have. Specify storage and memory requirements. |

|  |  |  |
| --- | --- | --- |
| **MacOS-App** | ⌇ | |
| **MacOS-Prog** | Vendor provides a native MacOS Application deployed independent of the Apple App Store | Offeror should document the capacities and limitations of the vendor supported MacOS Application relevant to the offering. Document any dependencies or requirements the software may have. Note if the application requires User level or System Administration level access to install. Specify storage and memory requirements. |
| **MacOS-Prog** | ⌇ | |
| **MacOS-Web** | Vendor provides a browser based service that is fully functional using Apple **Safari** under MacOS on an Apple MacBook device. | Offeror should document the capacities and limitations of the vendor supported web service relevant to the offering, when accessed via the Apple Safari browser on an Apple MacBook device. |
| **MacOS-Web** | ⌇ | |
| **MacOS-WebAlt** | Vendor provides a browser based service that is fully functional using an **alternate browser** under MacOS on an Apple MacBook device. | Offeror should document the capacities and limitations of the vendor supported web service relevant to the offering, when accessed via alternative MacOS browser on an Apple MacBook device.  Offeror should specify detailed browser compatibility specifications (Chrome, Firefox, etc.), versions currently supported, configuration or plug-in requirements. |
| **MacOS-WebAlt** | ⌇ | |
| **Win** | **Intel based Microsoft Windows Computers**  **(approx. ~5,000)** | **APS provides certain instructional programs with Intel based computers (either desktop or laptop) running Microsoft Windows OS.**  **APS also may provide MDM managed Windows Laptops classroom teachers and administrative staff** |
| **Win** | ⌇ | |
| **Win-Prog** | Vendor provides a native Windows OS Application | Offeror should document the capacities and limitations of the vendor supported Windows Application relevant to the offering. Document any dependencies or requirements the software may have. Note if the application requires User level or System Administration level access to install. Specify storage and memory requirements. |
| **Win-Prog** | ⌇ | |
| **Win-Web** | Vendor provides a browser based service that is fully functional using either Google Chrome, Mozilla Firefox, or Microsoft Edge browser on an Intel based device running Windows 10 or later. | Offeror should document the capacities and limitations of the vendor supported web service relevant to the offering, when accessed via supported browsers under Microsoft Windows OS.  Offeror should specify detailed browser compatibility specifications (Chrome, Firefox, etc.), versions currently supported, configuration or plug-in requirements. |
| **Win-Web** | ⌇ | |
| **iOS-iPhone** | Apple iPhones (ad Hoc) | APS does not deploy managed Apple iPhones for student or staff use, but some students or staff may utilize such **personal devices** to access the Offeror's services.  Offeror should provide information about iPhone functionality and support if available. |
| **iOS-iPhone** | ⌇ | |
| **Android** | Android Phones or Tablets (N/A) | APS does not generally deploy Android based devices, but some students or staff may utilize such **personal devices** to access the vendor's services.  Offeror may provide information about Android support if available. |
| **Android** | ⌇ | |
| **ChromeOS** | ChromeOS Devices (N/A) | APS does not generally deploy ChromeOS based devices (aka Chromebooks), but some students or staff may utilize such **personal devices** to access the vendor's services.  Offeror may provide information about ChromeOS support if available. |
| **ChromeOS** | ⌇ | |

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | **APS Service Platforms** | |
| **SIS-Synergy** | Synergy SIS | APS utilizes the ***Synergy*** Student Information System (SIS) provided by EduPoint for core SIS functions. |
| **SIS-Synergy** | ⌇ | |
| **ERP-Oracle** | Oracle ERP | APS utilizes the ***Oracle E-Business Suite*** of Enterprise Resource Planning (ERP) provided by Oracle for core HR and Finance functions. |
| **ERP-Oracle** | ⌇ | |
| **ID-Rapid** | Rapid Identity (SSO) | APS utilizes **Rapid Identity** by Identity Automation for Core digital identity, account management and authentication functions. |
| **ID-Rapid** | ⌇ | |
| **Azure365** | Microsoft 365/Azure | APS maintains a **Microsoft 365 / Azure** environment that provides various cloud services including email and SSO federation/authentication.  All Students and Staff are provided individual accounts in this environment. |
| **Azure365** | ⌇ | |
| **Google** | Google Workspace for Education | APS maintains a **Google Workspace for Education** environment that provides various cloud services including SSO federation/authentication.  All Students and Staff are provided individual accounts in this environment. |
| **Google** | ⌇ | |
| **ID-Clever** | Clever (Rostering & SSO) | APS maintains a **Clever** integration environment that provides centralized access to identity and enrollment (rostering) data.  Limited identity data for all Students and Staff is available via Clever data sharing subscription.  Limited SSO functionality is provided by Clever. This functionality is generally utilized by Elementary schools more than secondary schools. |
| **ID-Clever** | ⌇ | |
| **LMS-Canvas** | Canvas LMS | APS utilizes **Canvas** by Instructure for system-wide Instructional & Learning Management functions including Student-Teacher Communication, Assignment Tracking and LTI based integrations. |
| **LMS-Canvas** | ⌇ | |
| **MDM-AirWatch** | AirWatch MDM | APS utilizes the **AirWatch** MDM system for enterprise management of Apple iPads and MacBooks. |
| **MDM-AirWatch** | ⌇ | |
| **CRM-Zendesk** | Zendesk CRM | APS utilizes the **Zendesk** CRM system for internal (staff) and external (community) technology incident management and CRM functions. |
| **CRM-Zendesk** | ⌇ | |
| **BI-MicroStrat** | MicroStrategy Business Intelligence & Analytics | APS utilizes the **MicroStrategy** BI platform for Business Intelligence analysis and reporting. |
| **BI-MicroStrat** | ⌇ | |
|  |  |  |

|  |  |  |
| --- | --- | --- |
|  | **Network Environment** | |
| **APS-Network** | General Network | **Provide** specifications around network protocols used by the offering (example:IPv4/HTTPS)  **Provide** documentation on general network capacity required for normal use of offering including:   * A concise description of enterprise level network usage patterns for other organizations of equivalent size and scope to APS. * Expected average concurrent bandwidth requirements per user over a normal 15 minutes of use. |
| **APS-Network** | ⌇ | |
| **APS-Campus** | APS Campus | APS maintains a robust IPv4 based network in and between all schools and administrative buildings.  APS maintains a large capacity Internet connection that provides IPv4 Internet service to all schools and administrative buildings. |
| **APS-Campus** | ⌇ | |
| **APS-Wireless** | APS Wireless | APS provides a robust 802.11 wireless (Wi-Fi) network in and around all schools and administrative buildings.  All students and staff may access this network using their Wi-Fi capable APS provided client devices |
| **APS-Wireless** | ⌇ | |
| **Home-Internet** | Offsite Access / Home Internet | APS is committed to supporting staff and students wherever they need to work from. This includes accessing APS systems from their home or other remote locations via public Internet services.  **Note** any limitations or restrictions anticipated when accessing offering from high latency or low-bandwidth Internet services.  **Specify** if the offering is usable without active Internet access (i.e., Offline) |
| **Home-Internet** | ⌇ | |
|  |  |  |
|  | **Digital Identity, Authentication & Authorization** | |
| **ID-Data** | Identity Management | APS maintains the systems of record for staff and student account identity information. APS can provide unique identifier and attribute data to facilitate automated account management.  **Provide** data requirements and specifications for identity and account management.  **Provide** data requirements and specifications for class rostering management (if relevant)  **Complete** the "Digital Identity Authentication & Authorization Grid" to document offerings capabilities and requirements. |
| **ID-Data** | ⌇ | |
| **ID-Auto** | Identity Automation | Offerings should support standard integrations and **automated** processes whenever possible. |
| **ID-Auto** | ⌇ | |

|  |  |  |
| --- | --- | --- |
| **ID-Fed** | Identity Federation | Offerings should support standard authentication federations (**SSO**). Native passwords are discouraged. |
| **ID-Fed** | ⌇ | |
| **ID-Roles** | Role-Based Authorization | Offerings should support **Role-Based Authorization**.  Standard roles for "Student" and "Staff/Teacher" should be supported by default based on class rostering data (where relevant) |
| **ID-Roles** | ⌇ | |
| **ID-Admin** | Identity Administration | Roles capable of managing accounts, entitlements, or system configuration (i.e., System Administration) should be subject to higher standards of authentication and auditing. |
| **ID-Admin** | ⌇ | |
| **ID-DBA** | Data Administration | Roles capable of managing data imports, exports, or bulk manipulation (i.e., database administration) should be subject to higher standards of authentication and auditing. |
| **ID-DBA** | ⌇ | |
|  |  |  |

**Digital Identity, Authentication & Authorization Feature Matrix**

**Notes:**

Use the following matrix to designate what options, controls, and attributes the offering has in relation to Account Management, Authentication and Authorization. You may augment this matrix with detailed explanations of the specific entitlements or limitations of user roles defined in the offering.

Each cell in the matrix may be blank (not available), may contain an affirmation indicating feature availability, or may contain a reference to a more detailed elaboration.

Provide multiple tables if the offering is composed of multiple systems with different specifications.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Topic | Feature | Students | Staff /  Teachers | School  Administrators | IT System  Administration |
| **Federated Authentication**  (aka: Single Sign On) | Standards Based **SAML** Authentication |  |  |  |  |
| **Microsoft** Azure/365 SSO |  |  |  |  |
| **Clever** SSO |  |  |  |  |
| **Google** SSO |  |  |  |  |
| **LTI** Based Authentication (via **Canvas**) |  |  |  |  |
| **LDAP** Based Password Authentication |  |  |  |  |
| Standards Based **oAuth** Authentication |  |  |  |  |
| Accounts can be Disabled (Locally) |  |  |  |  |
| Accounts can have alternate Native Password Authentication (Local Authentication Override) |  |  |  |  |
| Other (Specify) |  |  |  |  |
| **Native Password Authentication**  (aka: Local Passwords) | Stored using irreversible encryption (i.e., one- way, salted hashes) |  |  |  |  |
| Enforceable Password Complexity |  |  |  |  |
| Self-Service Reset Available |  |  |  |  |
| Administrative Reset Available |  |  |  |  |
| Administrative Initiation of Password to known value on Account Creation |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Accounts can be Temporarily Disabled |  |  |  |  |
| Multi-Factor Authentication Supported  (Specify supported factors) |  |  |  |  |
| All Password Change Events are Logged, and User is Notified of Event |  |  |  |  |
| **Account Management & Rostering** | Manual Account Provisioning |  |  |  |  |
| Manual Rostering (Class Assignment) |  |  |  |  |
| Automatic Account Creation on first Authentication |  |  |  |  |
| **LTI** Based Account Provisioning (via **Canvas**) |  |  |  |  |
| **LTI** Based Roster Management (via **Canvas**) |  |  |  |  |
| **Clever** Account Provisioning Integration |  |  |  |  |
| **Clever** Roster Management Integration |  |  |  |  |
| Directory (**LDAP**) Based Account Provisioning |  |  |  |  |
| Automated Delimited File Processing (*OneRoster* Standard) |  |  |  |  |
| Automated Delimited File Processing (Clever Standard) |  |  |  |  |
| Automated Delimited File Processing (Custom CSV) |  |  |  |  |
| **REST API** Based Account Management |  |  |  |  |
| Other (Specify) |  |  |  |  |
| **Roles & Entitlements** | **Manual** Role Assignment |  |  |  |  |
| **Automatic** Role Assignment based on Rostering Data |  |  |  |  |
| **Fixed** Role Rights & Entitlements |  |  |  |  |
| **Configurable** Role Rights & Entitlements |  |  |  |  |
| Other (Specify) |  |  |  |  |

**Service Management & Support**

**Notes:**

The following table lists detailed expectations and requests for information on Offeror's service management policies and procedures including Maintenance, SLA's, and Support options.

Please provide inline responses in the lower sections marked with “ ⌇ “ or provide indexed auxiliary responses, notes, comments, or documentation using the "*APS Reference*" field as the cross-reference key.

|  |  |  |
| --- | --- | --- |
| APS Reference | Description | Notes |
|  | **Service Level Agreement** | |
| **SLA-Uptime** | Service Availability | System Availability should be available to a level of 99.9%, calculated over a 30-day period, 24/7, outside of regularly scheduled and communicated maintenance windows. |
| **SLA-Uptime** | ⌇ | |
| **SLA-Data** | Service Availability Record | Provide actual monthly availability for the previous school year. |
| **SLA-Data** | ⌇ | |
| **SLA-Sched** | Scheduled Maintenance / Downtime | Describe the communication policies and procedures for **scheduled** system outages/upgrades including timelines. |
| **SLA-Sched** | ⌇ | |
| **SLA-UnSched** | Un-Scheduled Downtime | Describe the communication policies and procedures for **unscheduled** service outages including timelines. |
| **SLA-UnSched** | ⌇ | |
| **SLA-Plan** | Maintenance Plan | Provide current yearly **planned maintenance schedule** and the schedule for at least one previous year. Offeror may provide schedules based on an academic school year or based on a calendar year. |
| **SLA-Plan** | ⌇ | |
| **SLA-Change** | Change Management | Describe the communication policies and procedures for Service Changes including changes to the User Interface, New Feature Introduction, Feature Removal/Depreciation. |
| **SLA-Change** | ⌇ | |
|  |  |  |
|  | **Support Model** | |
| **Support-SysAdmin** | Standard Technical Support | Offeror should provide support for **APS System Administrators** during regular business hours (M-F). Describe regular support business hours in Eastern time. |
| **Support-SysAdmin** | ⌇ | |

|  |  |  |
| --- | --- | --- |
| **Support-Weekend** | Extended Technical Support | If Offeror provides additional weekend support hours for end-users, describe. |
| **Support-Weekend** | ⌇ | |
| **Incident** | Incident Tracking | Offeror should provide a web-based incident tracking system, allowing designated APS support contacts to create and track system problems. Describe current incident tracking capabilities. |
| **Incident** | ⌇ | |
| **Escalation** | Problem Escalation | Offeror should provide a support escalation POC, contact information, and process. |
| **Escalation** | ⌇ | |
| **Support-User** | User Support | The Offeror should provide support contact information for **end users** using one or more of the following methods: |
| **Support-User** | ⌇ | |
| **Support-Phone** | Phone Support | User Support via Toll-free Telephone Help Desk / Call Center |
| **Support-Phone** | ⌇ | |
| **Support-Email** | E-mail Support | User Support via Email |
| **Support-Email** | ⌇ | |
| **Support-Chat** | Chat Support | User Support via Live Chat |
| **Support-Chat** | ⌇ | |
| **Support-FAQ** | Knowledgebase | Searchable knowledge base. Describe what tools and documentation are available and accessible online that provide training materials, support references, quick reference guides, or other items. |
| **Support-FAQ** | ⌇ | |
|  |  |  |
|  | **Disaster Recovery / Service Resiliency** | |
| **DR-General** | Disaster Recovery | Describe the overall disaster recovery / resiliency plan in place for the offering including: |
| **DR-General** | ⌇ | |
| **DR-Redundancy** | Redundancy | Redundancy |
| **DR-Redundancy** | ⌇ | |
| **DR-Backups** | Backups | Backups |
| **DR-Backups** | ⌇ | |
| **DR-Capacity** | Capacity Planning | Capacity Planning |
| **DR-Capacity** | ⌇ | |
| **DR-DoS** | Denial of Service (DoS) | Denial of Service (DoS) Mitigation |
| **DR-DoS** | ⌇ | |
| **DR-Ransomware** | Ransomware | Ransomware Mitigation & Recovery |

|  |  |  |
| --- | --- | --- |
| **DR-Ransomware** | ⌇ | |
|  |  |  |

**APS Service Provider: CIS Controls (v8.0)**

# Notes:

The following table references standards and practices from the **Center for Internet Security (CIS) Critical Security Controls Version 8.0** that Arlington Public Schools considers when evaluating Vendor's information technology products and services.

Please provide inline responses in the lower sections marked with “ ⌇ “ or provide indexed auxiliary responses, notes, comments, or documentation using the "*APS Reference*" field as the cross-reference key.

Indicate whether the offering conforms to these standards and practices and provide notes, elaboration, or evidence to substantiate your assertions of conformance. The level of conformity, completeness of response and level of substantiation will be considered in the evaluation of the offering.

HTTP references to **publicly available** online documentation is acceptable; specific location (page, section paragraph, etc.) should be specified.

Non-Disclosure Agreements (NDAs) that cover proprietary vendor technical information may be allowed.

## **REF:** See APS Policy “[M-12.4 Information Security](https://go.boarddocs.com/vsba/arlington/Board.nsf/files/BRHMMS56B7DF/%24file/M-12.4%20PIP-1%20Information%20Security%20Program.pdf)”

**REF:** <https://www.cisecurity.org/controls/v8/>

|  |  |  |
| --- | --- | --- |
| CIS Index | Safeguard | Description |
|  | **Data Protection** | |
| **CIS8-3.1** | Establish and Maintain a Data Management Process | Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the service. Review and update documentation annually, or when significant service changes occur that could impact this Safeguard. |
| **CIS8-3.1** | ⌇ | |
| **CIS8-3.2** | Establish and Maintain a Data Inventory | Establish and maintain a data inventory, based on the service’s data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data. |
| **CIS8-3.2** | ⌇ | |
| **CIS8-3.4** | Enforce Data Retention | Retain data according to the service’s data management process. Data retention must include both minimum and maximum timelines. |
| **CIS8-3.4** | ⌇ | |
| **CIS8-3.5** | Securely Dispose of Data | Securely dispose of data as outlined in the service’s data management process. Ensure the disposal process and method are commensurate with the data sensitivity. |
| **CIS8-3.5** | ⌇ | |

|  |  |  |
| --- | --- | --- |
| **CIS8-3.7** | Establish and Maintain a Data Classification Scheme | Establish and maintain an overall data classification scheme for the service. Services may use labels, such as “Sensitive,” “Confidential,” and “Public,” and classify their data according to those labels. Review and update the classification scheme annually, or when significant service changes occur that could impact this Safeguard. |
| **CIS8-3.7** | ⌇ | |
| **CIS8-3.8** | Document Data Flows | Document data flows. Data flow documentation includes service provider data flows and should be based on the service’s data management process. Review and update documentation annually, or when significant service changes occur that could impact this Safeguard. |
| **CIS8-3.8** | ⌇ | |
| **CIS8-3.9** | Encrypt Data on Removable Media | Encrypt data on removable media. |
| **CIS8-3.9** | ⌇ | |
| **CIS8-3.10** | Encrypt Sensitive Data in Transit | Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH). |
| **CIS8-3.10** | ⌇ | |
| **CIS8-3.11** | Encrypt Sensitive Data at Rest | Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data. |
| **CIS8-3.11** | ⌇ | |
| **CIS8-3.14** | Log Sensitive Data Access | Log sensitive data access, including modification and disposal. |
| **CIS8-3.14** | ⌇ | |
|  | **Continuous Vulnerability Management** | |
| **CIS8-7.1** | Establish and Maintain a Vulnerability Management Process | Establish and maintain a documented vulnerability management process for service assets. Review and update documentation annually, or when significant service changes occur that could impact this Safeguard. |
| **CIS8-7.1** | ⌇ | |
|  | **Audit Log Management** | |
| **CIS8-8.1** | Establish and Maintain an Audit Log Management Process | Establish and maintain an audit log management process that defines the service’s logging requirements. At a minimum, address the collection, review, and retention of audit logs for service assets. Review and update documentation annually, or when significant service changes occur that could impact this Safeguard. |
| **CIS8-8.1** | ⌇ | |
| **CIS8-8.11** | Conduct Audit Log Reviews | Conduct reviews of audit logs to detect anomalies or abnormal events that could indicate a potential threat. Conduct reviews on a weekly, or more frequent, basis. |
| **CIS8-8.11** | ⌇ | |
|  | **Malware Defenses** | |
| **CIS8-10.1** | Deploy and Maintain Anti-Malware Software | Deploy and maintain anti-malware software on all service assets. |
| **CIS8-10.1** | ⌇ | |
|  | **Data Recovery** | |

|  |  |  |
| --- | --- | --- |
| **CIS8-11.1** | Establish and Maintain a Data Recovery Process | Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant service changes occur that could impact this Safeguard. |
| **CIS8-11.1** | ⌇ | |
| **CIS8-11.3** | Protect Recovery Data | Protect recovery data with equivalent controls to the original data. Reference encryption or data separation, based on requirements. |
| **CIS8-11.3** | ⌇ | |
| **CIS8-11.5** | Test Data Recovery | Test backup recovery quarterly, or more frequently, for a sampling of in-scope service assets. |
| **CIS8-11.5** | ⌇ | |
|  | **Network Monitoring and Defense** | |
| **CIS8-13.1** | Centralize Security Event Alerting | Centralize security event alerting across service assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard. |
| **CIS8-13.1** | ⌇ | |
|  | **Application Software Security** | |
| **CIS8-16.2** | Establish and Maintain a Process to Accept and Address Software Vulnerabilities | Establish and maintain a process to accept and address reports of software vulnerabilities, including providing a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant service changes occur that could impact this Safeguard.  Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders. |
| **CIS8-16.2** | ⌇ | |
| **CIS8-16.7** | Use Standard Hardening Configuration Templates for Application Infrastructure | Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening. |
| **CIS8-16.7** | ⌇ | |
| **CIS8-16.13** | Conduct Application Penetration Testing | Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user. |
| **CIS8-16.13** | ⌇ | |
|  | **Incident Response Management** | |
| **CIS8-17.2** | Establish and Maintain Contact Information for Reporting Security Incidents | Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date. |
| **CIS8-17.2** | ⌇ | |

|  |  |  |
| --- | --- | --- |
| **CIS8-17.3** | Establish and Maintain a Process for Reporting Incidents | Establish and maintain a process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported. Ensure the process is publicly available to all of the workforce. Review annually, or when significant service changes occur that could impact this Safeguard. |
| **CIS8-17.3** | ⌇ | |
| **CIS8-17.4** | Establish and Maintain an Incident Response Process | Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan. Review annually, or when significant service changes occur that could impact this Safeguard. |
| **CIS8-17.4** | ⌇ | |
| **CIS8-17.6** | Define Mechanisms for Communicating During Incident Response | Determine which primary and secondary mechanisms will be used to communicate and report during a security incident. Mechanisms can include phone calls, emails, or letters. Keep in mind that certain mechanisms, such as emails, can be affected during a security incident. Review annually, or when significant service changes occur that could impact this Safeguard. |
| **CIS8-17.6** | ⌇ | |
|  | **Penetration Testing** | |
| **CIS8-18.1** | Establish and Maintain a Penetration Testing Program | Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the service. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements. |
| **CIS8-18.1** | ⌇ | |

**APS Service Provider: IT Security Standards**

**Notes:**

The following table references information technology standards and frameworks that Arlington Public Schools considers potentially relevant to evaluation of vendor offerings.

Indicate the vendor's status in relation to these standards and frameworks. Provide notes, elaboration, or evidence to substantiate the assertions in the lower sections marked with “ ⌇ “ or provide indexed auxiliary responses, notes, comments, or documentation using the "*APS Reference*" field as the cross-reference key.

**Vendor Adoption or Alignment:** Vendor has awareness of and utilizes standards for internal guidance and assessment

**Vendor Compliance or Assessment:** Vendor has documented conformity to standards (in part or in whole)

**Vendor Certification:** Vendor has third party certification of conformity to standards

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| APS Reference | Standard or Framework | Vendor Adoption or  Alignment | Vendor Compliance or  Assessment | Vendor Certification |
|  |  |  |  |  |
|  | **General** | | | |
| **PCI-DSS** | Payment Card Industry Data Security Standard (PCI DSS) |  |  |  |
| **PCI-DSS** | ⌇ | | | |
| **HIPAA** | Health Insurance Portability and Accountability Act (HIPAA) |  |  |  |
| **HIPAA** | ⌇ | | | |
| **COPPA** | Children's Online Privacy Protection Act (COPPA) |  |  |  |
| **COPPA** | ⌇ | | | |
| **GDPR** | European Union Law, General Data Protection Regulation (GDPR) |  |  |  |
| **GDPR** | ⌇ | | | |
| **ITIL** | Information Technology Infrastructure Library (ITIL) |  |  |  |
| **ITIL** | ⌇ | | | |
| **VSPA** | Virginia Student Privacy Alliance (SDPC)  [*Virginia School Data Privacy Agreement*](https://sdpc.a4l.org/agreements/VADPA-2020_SDPCv1a.pdf) |  |  |  |
| **VSPA** | ⌇ | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **SPP** | The Student Privacy Pledge  [*https://studentprivacypledge.org/*](https://studentprivacypledge.org/) |  |  |  |
| **SPP** | ⌇ | | | |
|  | **System & Organization Controls (SOC)** | | | |
| **SOC2-T1** | SOC 2 (Type 1) |  |  |  |
| **SOC2-T1** | ⌇ | | | |
| **SOC2-T2** | SOC 2 (Type 2) |  |  |  |
| **SOC2-T2** | ⌇ | | | |
| **SOC3** | SOC 3 |  |  |  |
| **SOC3** | ⌇ | | | |
| **SOC-Cyber** | SOC Cybersecurity |  |  |  |
| **SOC-Cyber** | ⌇ | | | |
|  | **Center for Internet Security (CIS)** | | | |
| **CIS7** | CIS Controls v7.x |  |  |  |
| **CIS7** | ⌇ | | | |
| **CIS8** | CIS Controls v8.x |  |  |  |
| **CIS8** | ⌇ | | | |
|  | **National Institute of Standards and Technology (NIST)** | | | |
| **NIST-CSF** | NIST Cyber Security Framework |  |  |  |
| **NIST-CSF** | ⌇ | | | |
| **NIST-PF** | NIST Privacy Framework |  |  |  |
| **NIST-PF** | ⌇ | | | |
| **NIST-800.53** | NIST 800-53 R5 (or R4) |  |  |  |
| **NIST-800.53** | ⌇ | | | |
|  | **International Organization for Standardization (ISO)** | | | |
| **ISO-27001** | ISO 27001 / ISO 27002 |  |  |  |
| **ISO-27001** | ⌇ | | | |
|  | **Other (Specify)** | | | |
|  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |