RFP Technical Requirements Checklist

This checklist outlines technical requirements for policy and technology compatibility. Vendors must address each item to enable the Department to fully assess suitability.

Item #	RFP Requirements
1	Provide a high-level conceptual network diagram with the following information: • source and destination systems with any known IP addresses • whether IP addresses are floating or paid • traffic direction and type • port usage and encryption status
2	Provide the solution’s data dictionary, including key data elements and definitions.
3	List the five most sensitive customer-relevant data fields stored in the solution.
4	Describe your release and maintenance approach, including governance, principles, release schedules (major, minor, hotfix), and supporting documentation.
5	Explain your managed hosting environment, including infrastructure components such as hardware, operating systems, networking, backup, failover, and disaster recovery.
6	Provide assurance that SAAS Solutions maintain an independent Tenant for the state’s use.
7	Provide evidence of IPS signatures and event logs are maintained and available for State validation upon request.
8	Describe your managed hosting services, including software and hardware installation, updates, patching, monitoring, performance tuning, backup and disaster recovery, and planned or emergency maintenance.
9	Provide assurance all supported operating systems and third-party applications are assessed for patches and patched as required.
10	Provide a description of active services, including web services, and the hardening standards applied.
11	Provide assurance of a comprehensive next generation endpoint security solution with machine learning capable anti-malware, abnormal detection, file integrity monitoring, log file monitoring, host-based intrusion detection, and file reputation scanning.
12	Provide assurance of auditing on hosts capturing all security related activities, the environment must maintain event logs for up to 7 years.
13	Provide assurance access to application data noted as restricted to only authorized database administrators.

Item #	RFP Requirements
14	Describe compatibility with (Identity Access Management) for authentication (OAUTH2, OpenIDC, SAML 2.0).
15	Describe how all internet-facing web front-end servers are protected by an enterprise WAF with coverage for OWASP Top 10 risks, botnets, DDoS attacks, and virtual patching.
16	Provide details on how the application communication from users and across components of the application are encrypted (include details related to end users and/or staff remote access).
17	Describe how application security–related events, including logins, configuration changes, and administrative actions, are logged and reviewed for malicious or anomalous activity
18	Provide assurance that application code is scanned at least annually and prior to deployment of any changes into production.
19	Provide assurance that application undergoes dynamic scanning at least annually and prior to production changes.
20	Describe the method System Administrators are notified within 24 hours when third-party software releases are known to impact the current vendor software version.
21	Describe your approach to the installation and configuration of all software, hardware, and cloud services required to deliver a complete, working environment that meets initial performance requirements for the centralized web and mobile user interface and supports integration with the State of Delaware Master Data Management and Customer Agency applications. If cloud computing is used, explain how cloud resources are utilized, configured, maintained, and updated.
22	Provide a description of your approach to providing ongoing post-deployment support, maintenance, and upgrades.
23	Describe your approach to operating, maintaining, and administering the centralized web and mobile user interface on a 24×7×365 basis, including customer service, infrastructure, security, performance monitoring, software currency, standards compliance, and administrative management. Include details on: • Operations include customer service, facilities, hardware, networking, security, performance monitoring, and problem resolution. • Maintenance includes keeping all off-the-shelf software on current releases and keeping the development environment on mainstream industry and State accepted standards. • Administration includes all financial, record keeping, reporting, and management aspects of the platform.
24	Describe the solution's usability and compatibility across current versions of Microsoft Edge, Google Chrome, Mozilla Firefox, and Safari on desktop and mobile platforms, including supported operating systems, devices, and assistive technologies. Include applicable VPATs or accessibility assessments and plans to validate usability during development and prior to deployment.

Item #	RFP Requirements
25	Provide a copy of any 3rd party security framework certificates including but not limited to any of the following: • Internal Revenue Service Publication 1075 Compliance • NIST 800-53 • Information Security Management System 27001 (ISO 27001) • CSA STAR – Cloud Security Alliance – Security, Trust & Assurance Registry • Federal Risk and Authorization Management Program (FedRAMP) certification for a System hosted in a cloud environment • PCI DSS Compliance • Health and Human Services Health Insurance Portability and Accountability Act (HIPAA) Compliance
26	Provide the latest 3rd party audit or assessment report(s): • System and Organization Controls 2 (SOC-2) • Statement on Standards for Attestation Engagement 18 (SSAE-18) • PCI Report on Compliance (ROC) • Standardized Control Assessment (SCA) • Cybersecurity Maturity Model Certification (CMMC) Readiness Assessment
27	Provide a description of compliance and/or certificate showing how the vendor and proposed solution complies with: • Family Educational Rights and Privacy Act (FERPA) • Children's Internet Protection Act (CIPA) • Children's Online Privacy Protection Rule (COPPA) • Voluntary Product and Accessibility Template (VPAT)
28	Describe the firewall or next-generation network security controls implemented to enforce logical separation between architectural layers.
29	Describe how firewall rules are justified, documented, and specifically defined to meet application needs.
30	Describe how all database systems implement encryption beyond the default host-level encryption.
31	Describe how all API integrations accessing state data routes through the State API Gateway and comply with OWASP Top 10 and XML security controls.
32	Describe how all source network IPs, client certificates, and database queries are authenticated and validated using enforced security controls.
33	Describe how unique database access credentials are established for all users and how they are managed, reset, and revoked.
34	Describe the security incident detection and response management including: • Log collection, correlation, and threat intelligence • 24x7, 365 active security event monitoring and attack response • Compliance aligned with log retention • Log forwarding to Security Information and Event Management (SIEM) system

Item #	RFP Requirements
35	Provide assurance system vulnerability scans are performed and remediated at least quarterly. The state may request summaries of all assessments performed against the environment.
36	Provide assurance the system undergoes external penetration testing at least annually and provide report, upon request, with summaries of test scope, results, and remediation activities.
37	Explain how emergency service tickets are handled outside of normal business hours.
38	Explain the process and timelines for notifying customers of security threats or breaches.
39	Provide assurance the solution supports operation on mobile devices in compliance with the State's Mobile Device encryption protocols.
40	Provide assurance the solution is a highly available, fully web-based, and accessible via a standard web browser for its user interface with at least 256-bit encryption.
41	Provide assurance the system utilizes a scalable, industry-standard relational database management system (RDBMS), preferably an enterprise-proven SQL database system that supports real-time user access to critical data.
42	Provide assurance the system utilizes a single, highly available, centralized relational database management system (RDBMS) for all schools within the district.
43	Provide assurance the system relational database management system (RDBMS) includes integrated data backup and recovery capabilities and supports restoration of pre-rollover database versions.
44	Provide assurance the system relational database management system (RDBMS) includes the use of multiple online log files for data recovery, rollback capabilities, and auditing.
45	Provide assurance the system relational database management system (RDBMS) should enable locking of records to prohibit simultaneous updating by multiple users while still allowing multiple users to view the record.
46	Describe the method and frequency for monitoring and inventorying authorized and unauthorized users, devices, and software.
47	Provide assurance the solution utilizes a three-tier architecture or n-tier application model that separates processing across discreet tiers with clear separation of client, application, and data tiers.
48	Describe how the solution supports horizontal scaling to accommodate growth and workloads.
49	Describe how the solution supports vertical scaling to accommodate growth and workloads.
50	List the programming languages on which the system is built.

Item #	RFP Requirements
51	Provide assurance the solution supports use of non-production environment(s) and current documented data replication procedures are maintained for replicating data from the production instances.
52	Provide assurance the solution supports all major browsers including Edge, Firefox, Chrome, Safari without the use of browser 'plug-ins'.
53	Provide assurance the solution must allow 'back end' access to the database using SQL Developer Tools, ODBC, JDBC.
54	Provide assurance the solution supports native mobile apps across both Android and iOS with adaptive design for mobile functionality.
55	Provide assurance the solution is fully compatible for end user access across both MacOS and Microsoft Windows based platforms.
56	Provide assurance the hosted solution datacenter utilizes isolated-parallel (IP) UPS topology to provide resilient power protection.
57	Provide assurance the hosted solution datacenter complies with ASHRAE standards for temperature and humidity standards.
58	Provide assurance the hosted solution datacenter utilizes a Tier 1 Carrier Internet backbone with a minimum 10 Gigabit Ethernet connection for Internet connectivity.
59	Provide assurance the hosted solution datacenter utilizes a minimum combination of biometric scanners and card readers for physical access to the systems' infrastructure.
60	Provide assurance the hosted solution datacenter utilizes 24x7x365 internal and external CCTV video surveillance that includes a minimum 90-day video retention policy.
61	Provide assurance the hosted solution incorporates XTS-AES at least 256-bit (or greater) encryption for data at rest to protect data confidentially.
62	Provide assurance the hosted solution incorporates CA-signed certificates with SHA-2 hashing and at least 256-bit cryptographic strength.
63	Describe how the hosted solution utilizes next-generation firewall (NGFW) technology with integrated intrusion detection system (IDS).
64	Describe how the hosted solution is protected by perimeter-based Distributed Denial of Service (DDoS) prevention and mitigation controls.
65	Provide assurance the hosted solution's redundant backup levels incorporate daily full backups and offsite storage with a minimum 30-day retention policy.
66	Provide assurance the hosted solution maintains multiple online log files across multiple redundant disks and/or SAN LUNs.
67	Describe the Disaster Recovery plan including offsite recovery location and a Data Continuity plan listing the Recovery Point Objective (RPO) in the event the primary systems become unavailable or unresponsive.

Item #	RFP Requirements
68	Describe how the hosted solution supports a unique, secure, and fully isolated instance for each district.
69	Provide assurance the hosted solution will sustain 99.9% uptime excluding planned outages and supports system restoration within one hour.
70	Provide assurance the solution supports outbound traffic routing through the State of Delaware proxy system (wwwproxy.k12.de.us:8080)
71	If an on-premises solution is proposed, provide assurance the on-premises hosted solution installation on Windows Server 2019 and greater or Windows Server Virtual Machines (VMWare ESXi) or via VMware OVF Appliance and can integrate with Delaware's cloud-based Student Information System without the need to depend on Docker or Kubernetes.
72	Provide assurance the proposed solution uses Microsoft SQL Server as its RDBMS, with SQL Server 2019 as the minimum supported version.
73	Describe the connectivity methods and data transfer capabilities to exchange data between solution and student database.
74	Attach signed Conditions Governing Cloud Services and Data Usage Agreement
75	Include in the agreement to permit Department-level audit to be reviewed based on the components within this checklist and/or regulated items handed down to the Department
76	Provide experience of the staff that will be working with the Department on implementing the solution
77	List all cybersecurity committees or Information Security and Analysis Center (ISAC) participation (IT-ISAC, FS-ISAC, CISA, etc)
78	Agree to work with the Department and the State to develop approved detailed network design for implementation