

Licensing RFP System Requirements - Iowa DIAL - 2023 - Appendix A

Licensing RFP System Requirements - Iowa DIAL - 2023 - Appendix A				Vendor Response
Number	Requirement Type	Weight	Requirement Detail	
4.4.5.1	Accessibility	10	The application must meet or exceed current WAI WCAG AA compliance standards this includes 2.x and 3.x. The application must maintain current documented standards throughout the application lifecycle.	
4.4.5.2	Accessibility	10	The application must meet all State of Iowa and Federal Accessibility standards.	
4.4.5.3	Accessibility	10	The application must be responsive on any standard desktop, mobile or tablet device.	
4.4.5.4	Accessibility	8	The application must support users on high latency and/or low bandwidth connections. Graceful degradation is allowed to meet performance objectives. Note: this would include connections to mobile devices and/or satellite connections which are common among rural constituents. This performance must be demonstrated.	
4.4.5.5	Accessibility	8	The application must support any consumer or enterprise browser with marketshare over 5% throughout the life of the project. Note this currently would include Chrome, Edge, Safari and Firefox. Additional information.	
4.4.5.6	Administrative	8	The system must support a wide variety of reporting, including equivalency of all current reporting.	
4.4.5.7	Administrative	9	Individual users must have the ability to create and design reports without development resources or the use of code.	
4.4.5.8	Administrative	10	The system must support the creation of new applications and workflows without the need for development and/or engineering staff.	
4.4.5.9	Administrative	10	Trained internal business stakeholder(s) must be able to create and modify existing application(s) and workflow(s) without vendor support.	
4.4.5.10	Administrative	10	The application workflows and forms must support conditional logic (or equivalent). Both workflows and forms must be configurable via the application interface (UI).	
4.4.5.11	Administrative	10	Forms must support a wide variety of configurable field(s), variable(s) and data type(s) as needed to support licensing, permitting and inspection functionality.	
4.4.5.12	Administrative	10	Forms must support calculation.	
4.4.5.13	Administrative	10	The system must support the ability to obfuscate field level data.	
4.4.5.14	Administrative	10	The system must support the ability to support 3 part forms.	
4.4.5.15	Administrative	10	The system must support forms which require multiple signatures.	
4.4.5.16	Administrative	10	The system must allow for routine audits and all appropriate and necessary access as required by law, statute or administrative need.	
4.4.5.17	Administrative	10	If the system utilizes 3rd party reporting tools you must describe the approach, tool(s) used and any potential concerns.	
4.4.5.18	Administrative	10	If a programmatic language is used in reporting you must describe which languages are supported and/or used.	
4.4.5.19	Administrative	10	The application Vendor must identify the tools used to create forms; whether the tool is built into their product or is an add-on, please describe.	
4.4.5.20	Analytics	10	The application must allow the use of Google Tag Manager (GTM).	
4.4.5.21	Analytics	10	Google and other analytics tools must be integrated via Google Tag Manager.	
4.4.5.22	Analytics	10	The application must allow integration with third party analytics providers and custom code providers (this requirement can be fulfilled via Google Tag Manager).	
4.4.5.23	Analytics	6	Analytics must be provided on a per license basis and must incorporate conversion tracking for common application actions such as completion, rejection, etc.	
4.4.5.24	Analytics	8	The vendor must provide initial and ongoing benchmarking and reporting (or access) on a regular basis as it relates to application completion, abandonment and other relevant factors as defined by business need.	
4.4.5.25	Architecture	10	The vendor is directly responsible for all network and server infrastructure. This infrastructure must be maintained and show continuous evidence that the application stack is current and patched per State of Iowa and OCIO security policy.	
4.4.5.26	Architecture	10	The application infrastructure must be standalone with no dependencies tied to any other 3rd party client or existing vendor business partner or third party implementation.	
4.4.5.27	Architecture	10	The application codebase must be standalone with no dependency on any other business or government entity.	
4.4.5.28	Architecture	8	The application architecture must be flexible and allow for core updates as well as customization. Customization must not negatively impact the ability to perform core product updates.	
4.4.5.29	Architecture	10	The system must support full on demand system backups as well as incremental backups.	
4.4.5.30	Architecture	8	The application vendor must provide a written backup plan that is agreed upon by all relevant parties.	
4.4.5.31	Architecture	8	The vendor must provide development, test and production environments. Those environments must be synchronized on a standard consistent basis (bonus if this done daily).	
4.4.5.32	Architecture	10	Data must be accessible via standard API interfaces for all out-of-the-box promised functionality and/or as agreed upon by both parties, please provide details.	
4.4.5.33	Architecture	10	Data must be portable with interfaces and/or processes which allow us to consume or export system all system data on demand or request.	
4.4.5.34	Architecture	8	The application must support continuous integration.	
4.4.5.35	Architecture	8	The application must be extensible with a wide variety of available integrations for enhanced functionality.	
4.4.5.36	Architecture	10	The application must support scheduled and on-demand data (feed) ingestion and export with all existing internal and external partners including the federal government.	
4.4.5.37	Architecture	5	The system must support 3rd party identity verification service(s).	
4.4.5.38	Clawback	10	Failure to meet SLA's and uptime obligations must result in an equivalent offset of software support and licensing costs.	
4.4.5.39	Core	10	Reliability: The software must be reliable and perform consistently under different conditions.	
4.4.5.40	Core	10	Scalability: The software must be able to handle an increasing amount of data or users without compromising performance.	
4.4.5.41	Core	10	Security: The software must be secure and protect against unauthorized access or data breaches.	
4.4.5.42	Core	10	Usability: The software must be easy to use and navigate for the intended users.	
4.4.5.43	Core	10	Compatibility: The software must be compatible with different operating systems, hardware, and other software.	
4.4.5.44	Core	10	Maintainability: The software must be easy to maintain and update over time.	
4.4.5.49	Data Migration	10	The vendor must be responsible for field mapping and review.	
4.4.5.50	Data Migration	10	The vendor must be responsible for migrating all data from prior existing applications into the new system. This includes includes all necessary staff and resources for migrating data from prior licensing application / software instances that are currently supported by the State of Iowa. This will include instances of Amanda, Image Trend, Salesforce, etc. This is subject to acceptance testing and validation (please describe).	
4.4.5.51	Design	10	The application platform must meet current DIAL, State of Iowa (OCIO) and Federal Design Standards.	
4.4.5.52	Design	8	The application must use a standard design framework and web components (please describe).	
4.4.5.53	Design	8	The application must be designed to meet plain language standards see (https://www.plainlanguage.gov).	
4.4.5.54	Documentation	10	The application must be documented to a level which allows system restoration independent of the implementation partner.	
4.4.5.55	Documentation	10	User manuals and/or online documentation must be provided and include role specific and citizen specific instructions on system functionality as appropriate.	
4.4.5.56	Documentation	10	Administrative user manuals and documentation must be provided which outlines detailed instructions on system infrastructure, administrative and configuration.	
4.4.5.59	Documentation	10	The vendor must provide a data flow diagram.	

Licensing RFP System Requirements - Iowa DIAL - 2023 - Appendix A

Number	Requirement Type	Weight	Requirement Detail	Vendor Response
4.4.5.60	Other	10	The system must support all common case management functionality as necessary to support inspections.	
4.4.5.61	Other	10	The application must support broad continuing education functionality for licensees, training providers and administrative staff (please describe).	
4.4.5.62	Other	10	The application must support plan review functionality.	
4.4.5.63	Other	10	Public View, the application must support search and view functionality of licensing information where appropriate and required by Statute or Law.	
4.4.5.64	Other	10	The application must support ALL existing licensing, permitting and related inspection functionality as currently deployed at DIAL.	
4.4.5.65	Payments	10	The system must be able to support a wide variety of payment and accounting functionality. This includes third party billing, multiple payments. Payment functionality will be subject to user acceptance testing. Business users must be able to define payments which can be directed to specific accounts and/or buckets as applicable.	
4.4.5.66	Payments	10	The application must support a variety of third party integration with external payment providers, our current provider is US Bank.	
4.4.5.67	Payments	10	The system must allow user payments to be refunded by staff with appropriate roles.	
4.4.5.68	Payments	10	Payments and accounting functionality must be integrated with state supported systems (please describe).	
4.4.5.69	Performance	10	The application must exhibit no visible latency (less than 100ms). User acceptance testing will be required to validate performance. This is a requirement throughout the life of the agreement.	
4.4.5.70	Performance	10	Google page speed insights (or other applicable and/or equivalent tooling) must show key application performance indicators in the green (90+) for both desktop and mobile.	
4.4.5.71	Performance	10	The application must scale to seamlessly accommodate surges in user activity without any noticeable degradation in performance.	
4.4.5.72	Performance	10	The web application must meet key web application performance standards (KPI's) as defined by the OCIO.	
4.4.5.73	Performance	10	The system must have the ability to handle simultaneous automated processes & integrations without degradation in reasonable performance measures.	
4.4.5.74	Project	10	Weekly summary updates must be provided to all relevant leadership and stakeholders during the development process. This should include but not limited to a bi-weekly demo of system functionality while the application is development.	
4.4.5.75	Project	10	The vendor must provide resources to analyze current application processes and be equipped to standardize and manage all 280+ application, licensing and inspection processes currently supported via DIAL. A list of all licensing, permitting and application application processes is available for review.	
4.4.5.76	Project	7	The vendor must provide training resources utilizing a variety of delivery methods through the life of the agreement. Initial onsite training, ongoing training and workshops where appropriate.	
4.4.5.77	Project	10	The vendor must provide all necessary support for business process-reengineering, leveraging LEAN methodology.	
4.4.5.78	Project	10	Application development and project implementation must be conducted using agile methodology (please describe).	
4.4.5.79	Reliability	10	The system must maintain availability of 99.99% as a core requirement (52 minutes of downtime per year).	
4.4.5.80	Reliability	10	The application must never have downtime exceeding 24 hours (if you can guarantee less downtime, we will weigh this factor).	
4.4.5.81	Reliability	10	Disaster Recovery (DR) testing must be done at a minimum every 12 months. This includes a physical cut over of services from a primary to secondary independent application instance.	
4.4.5.82	Reliability	10	The application must run simultaneously in multiple independent data centers (geographically distinct).	
4.4.5.83	Reliability	10	Application data must be saved upon entry at the page and/or field level. In the event of a service outage an application can be resumed by the end user with a minimal amount of required rework.	
4.4.5.84	Reliability	7	Billable charges must be reduced accordingly by percentage in the event of a service outage.	
4.4.5.85	Security	10	All relevant staff working in the system are subject to standard state security screening and background check procedures upon request.	
4.4.5.86	Security	10	Administrative access to the system must be restricted by geography and specific IP ranges as authorized by DIAL and the State of Iowa.	
4.4.5.87	Security	10	All staff must be located in the United States.	
4.4.5.88	Security	10	Data, including backups, must be processed, stored, transmitted or accessed only in the Continental United States.	
4.4.5.89	Security	10	The application must be FEDRAMP compliant.	
4.4.5.90	Security	10	The application must maintain FEDRAMP High Authorization.	
4.4.5.91	Security	10	The application must meet all OCIO security policies, standards and rules as defined and documented via ocio.iowa.gov. Note: a security resource will be provided and available via the OCIO throughout the duration of this project.	
4.4.5.92	Security	10	The system must support all current and future user role(s) and allow for configuration and customization of role based access.	
4.4.5.93	Security	10	Known security vulnerabilities must be mitigated according to industry best practices, based upon the level of threat, the vendor is responsible for informing DIAL and the OCIO of any security vulnerability, mitigation effort(s) and outcomes. Vulnerabilities must be resolved in a timely manner.	
4.4.5.94	Security	10	Incidents involving exposure of licensing application data must be reported to the State of Iowa within 1 hour of discovery. Please describe.	
4.4.5.95	Security	10	The application must support field level encryption to FEDRAMP standards. Please detail which standards you currently meet (FIPS 140-x).	
4.4.5.96	Security	10	The system must support OKTA integration.	
4.4.5.97	Security	10	The application must support multifactor authentication (MFA) (satisfied by OKTA and/or other third party providers as approved via the OCIO).	
4.4.5.98	Security	10	The system must broadly support third party integration for automatic 3rd party user identity validation and fraud detection/prevention.	
4.4.5.99	Security	10	The application must be behind an OCIO approved WAF (Web Application Firewall).	
4.4.5.100	Security	10	The system must support the ability to obfuscate field level data.	
4.4.5.101	Security	10	The application must encrypt data in transit and at rest (DARE).	
4.4.5.102	Security	10	A SOC 2 report must be provided before production system go-live and annually after product launch.	
4.4.5.103	Security	10	The application must collect system log data. The system must support the ability to forward logged data to the State of Iowa's SEIM.	
4.4.5.104	Standards	10	The application must meet all current State policies, rules and application standards as defined by the OCIO and DIAL. Documentation is available via ocio.iowa.gov.	
4.4.5.105	Support	10	The vendor must agree to abide by a standard service level agreement(s) as defined in writing by both parties. This service level agreement must be in writing, easily available to all parties and reviewed on an annual basis (please describe).	
4.4.5.106	Support	10	The vendor must provide support staff available 24/7, 365 days per year for system support. Escalated support staff must be available on an on-call basis.	
4.4.5.107	Support	10	The time to respond to an emergency impacting multiple users must not exceed xx hours (please describe, baseline required minimum of 12 hours).	
4.4.5.108	Support	10	The vendor must provide a hotline for emergency technical support.	
4.4.5.109	Support	10	All vendor resources and contract staff must be US based within the contiguous United States.	
4.4.5.110	Technical	10	The vendor must not impose storage limitations (please describe any reasonable technical limitations).	
4.4.5.111	Technical	10	The vendor must support 3rd party storage options.	

Licensing RFP System Requirements - Iowa DIAL - 2023 - Appendix A

Licensing RFP System Requirements - Iowa DIAL - 2023 - Appendix A				Vendor Response
Number	Requirement Type	Weight	Requirement Detail	
4.4.5.112	Technical	10	The application must support virtually all available commercial file types, batch file upload, and large files including video, audio, plan and image files.	
4.4.5.113	Technical	10	The application must meet current state and industry coding standards as defined by the appropriate governing body. The goal being compliant, standardized, reviewable code.	
4.4.5.114	Technical	10	The vendor must meet current state and industry standards for HTML5+, CSS, JS and any other platform specific language that's being used during implementation. Please describe all languages used.	
4.4.5.115	Technical	10	On-demand monitoring of system resources and performance data must be available (please describe).	
4.4.5.116	Technical	10	The application must support universal search and "fuzzy" search functionality which would include all current and historical application data including the ability to search documents.	
4.4.5.117	Technical	10	The application must have the ability to send unlimited notifications via text, email or voice - notifications should be customizable by the end user (please describe).	
4.4.5.118	Technical	10	The application stack must support all current connections to external organizations and/or federal agencies via API based approaches.	
4.4.5.119	Technical	10	The system must support common geographic and mapping functionality as it relates to inspections and permitting (please describe).	
4.4.5.120	Technical	10	The system must support all currently used external integrations.	
4.4.5.123	User Experience	8	The vendor must prioritize usability issues (please explain).	
4.4.5.124	User Experience	8	The vendor must include feedback and support mechanisms for customers, staff and constituents (please describe).	
4.4.5.125	User Experience	8	The application must pass user acceptance testing (UAT) and validation internally before deployment.	
10/4/2023 - v2 - State of Iowa - DIAL				
RFP Number: RFP #1023-481-01				