

REQUEST FOR PROPOSALS

Coordinated Records Management, Public Records &
Website Modernization

Snohomish County Fire District 4

Issue Date: August 14th, 2026

**Proposals Due: September 25, 2026 by 5:00 PM
PT**

1. Project Context

Snohomish County Fire District 4 (The District) is a three-station fire district serving a portion of Snohomish County, Washington. The District is requesting proposals for a coordinated solution that modernizes three closely related areas of District operations: internal records management and filing, public records request processing, and the District's public website. The selected approach must also provide reliable local backup of District data independent of the vendor's cloud environment. These functions are being procured together because they create, receive, publish, locate, and retain overlapping District information. Website forms may create public records; approved records may need to be published online; and records requests submitted through the website must flow into an internal review process. The District is not requiring that every function be delivered through one software product. It is seeking one understandable, coordinated solution in which the components work together where appropriate and one prime vendor remains accountable for the overall result.

The District's core objectives are to:

- Create a dependable and understandable filing environment for current and legacy District records;
- Improve public records request intake, search, review, redaction, response preparation, production, deadline tracking, and audit documentation;
- Provide a modern, accessible public website that serves the entire District and gives residents clear access to information, services, forms, and public records request intake;
- Maintain secure, recoverable District data through cloud services and regular local backups under District control; and
- Retain meaningful human review and decision-making throughout records filing, classification, retention, public records review, exemption analysis, redaction, and production. Automation and artificial intelligence may assist staff, but shall not independently make final filing, deletion, disclosure, withholding, or redaction decisions.

The District has identified several possible public-service features, including an address-based outdoor burning information tool. These examples illustrate desired capabilities but are not intended to define the entire website or prescribe the final technical design. Vendors are invited to present a clear solution that meets the core objectives and identifies practical options, assumptions, limitations, and opportunities for phased implementation.

2. Purpose

The purpose of this RFP is to obtain proposals that present a clear, practical, and understandable solution to the District's core objectives. The proposed solution should reduce dependence on individual staff knowledge, improve the organization and retrieval of current and legacy records, strengthen public records compliance, protect sensitive information, provide independent local backup, and give residents a clear and accessible website for District information and services.

The records management system, public records request workflow, website, employee portal, and backup environment may remain distinct functional components, but they must exchange information where appropriate. For example, a request submitted through the website should enter the public records workflow without manual re-entry; approved public documents should be publishable from a controlled records source; and records created through website forms or registrations should be retained according to applicable schedules.

This RFP is intentionally outcome-focused and broad. The District does not expect vendors to resolve every workflow, configuration, field, integration, or implementation detail in their proposals. The

selected vendor will conduct structured discovery with District stakeholders after selection to define detailed requirements, priorities, phases, and configuration. Proposals should therefore explain the recommended approach in plain language, demonstrate how it satisfies the core objectives, identify material assumptions or exclusions, and describe how the solution can be refined during discovery. The District is open to a single product, a coordinated suite of products, or a vendor-managed combination of technologies, provided the proposed solution functions cohesively and maintains clear accountability.

2.1 Definitions

Coordinated Solution: The complete vendor-proposed approach for satisfying the District’s core objectives. It may consist of one product or multiple integrated technologies managed under one prime vendor.

District divisions: The various distinct units within the organization that share a common role (e.g., finance, operations, training, etc.)

Human-in-the-Loop: A required workflow in which authorized District personnel review, correct, approve, or reject system-generated classifications, recommendations, searches, redactions, retention actions, and draft responses before a final action occurs.

Records Management and Filing System: The internal tools and processes used to classify, organize, index, search, secure, retain, place legal holds on, and disposition District records.

Public Records Request System: The tools and workflow used to receive, track, search, review, redact, correspond about, and produce records responsive to requests under chapter 42.56 RCW.

Legacy Records: Existing records that may be stored in older systems or formats or may be scanned, poorly named, inconsistently filed, duplicated, or missing reliable metadata.

Local Backup: A regularly created, encrypted, usable copy of District data stored on District-controlled physical or on-premises media and recoverable without dependence on the vendor’s active cloud service.

Website: The District’s public-facing information and service portal. Public records request intake is one website function, but the website is intended to serve all District divisions and community audiences.

Artificial Intelligence or Automated Tools: Technology that assists with searching, classification, extraction, drafting, issue identification, or recommended actions. Such tools are advisory and do not replace District judgment or approval.

3. Scope of Work

The selected vendor will be responsible for proposing, delivering, and coordinating a solution addressing the following five project components. The descriptions below identify required outcomes and general capabilities; they are not intended as a complete technical specification:

- A records management and filing system that assists with classification, indexing, search, retention management, permissions, and audit history for current and legacy records, while requiring authorized human review for final classification, filing, retention, deletion, and legal-hold decisions;
- A public records request system that supports online intake, deadline tracking, responsive-record searches, review, suggested redaction, correspondence, production, and audit documentation, with a required human-in-the-loop workflow and explicit staff approval before any disclosure, withholding, redaction, or response is finalized or transmitted;
- A modern, mobile-friendly public website serving all District divisions, residents, businesses, and community partners;

- Migration and organization of existing digital records, including legacy records that may have limited or inconsistent metadata; and
- A mobile-friendly internal employee portal or intranet, as described in Section 4.6.

The solution shall use secure cloud hosting for normal operations and shall also include regular local backup of District data to District-controlled physical or on-premises storage. Local backup shall not depend on continued availability of the vendor's cloud environment and must be usable for recovery or transition if cloud services become unavailable.

The District prefers one prime vendor to remain accountable for coordination, implementation, integration, support, and successful operation of the complete solution. Subcontractors or third-party products may be used, but they must be clearly identified and managed by the prime vendor. The District should not be required to coordinate separate vendors to make the proposed components work together.

4. Website Requirements

4.1 Structure and Navigation

The Honolulu Fire Department website should serve as a reference for the website's navigation structure and the organization of website sections. Griffin Fire Department is another reference site identified by the District. The following list reflects currently identified needs and is not intended to be exhaustive. Final navigation, content, and service features will be developed through stakeholder discovery with all District divisions. The website shall be capable of including:

- Mobile-friendly responsive layout
- Fire Marshal section similar in structure to the Honolulu Fire Department
- Permits navigation section
- Community Risk Reduction section
- Public records request entry connected to the records management system
- Board meeting documents access. Records published through this section must remain exportable and retainable consistent with Washington public records retention requirements. Example of such items (Board resolutions, meeting minutes, adopted documents, inter-local agreements)
- Recruitment section
- Public FYI section covering high-traffic topics such as burn permits, inspections, public records requests, emergency contacts, seasonal safety information, and other common community questions
- Wildfire preparedness and seasonal safety content hub, including links to current Snohomish County evacuation zones, DNR fire restrictions, and defensible space resources

The platform shall support posting and public access to interlocal agreements (ILAs) entered into by the District. Under RCW 39.34.040, the District is required to either file each signed ILA with the county auditor or post it on its website or other electronically retrievable public source. Failure to properly file or post an ILA may affect its legal validity. The records management system shall treat ILAs as a named document category, support version control and date tracking for each agreement, and make current ILAs publicly accessible through the website. The system shall also flag ILAs approaching expiration for staff review.

4.1.1 Divisional Requirements and Stakeholder Input

The navigation structure and content architecture described in Section 4.1 reflects the District's current understanding of its public-facing and operational needs. All District divisions and offices will have content, workflow, and public-interface requirements that must be incorporated into the final platform design.

The following divisions and roles represent the District's currently identified needs. This list is not exhaustive, and the final website structure may include additional sections, services, workflows, or stakeholder groups identified through the vendor's discovery process and ongoing collaboration with the District. The selected platform must be flexible enough to accommodate evolving organizational needs and future opportunities to better serve the community.

- Operations: Station information, apparatus, staffing, and public emergency information
- Fire Marshal's Office: Permits, inspections, code enforcement information, outdoor burning guidance, fee information, forms, and future public-facing inspection and permit workflows
- Records Management and Public Records: Public records request intake, request tracking, records access, retention-related information, required public postings, and internal records-management workflows
- Employee Resources and Internal Communications: Secure access to policies, procedures, forms, announcements, training materials, operational documents, and other intranet resources for District personnel
- Finance: Budget documents, financial reports, levy information, and public financial disclosure postings
- Medical Services Officer: EMS program information, training resources, and community health initiatives
- Logistics: Procurement notices, vendor information, and supply-related public postings where applicable
- Safety Officer: Safety program information, incident reporting resources, and public safety notices
- Board of Fire Commissioners: Meeting agendas, minutes, resolutions, adopted documents, and commissioner contact information
- Citizens Advisory Board: Meeting information, member rosters, reports, and public participation resources
- Human Resources and Recruitment: Job postings, application processes, benefits information, and volunteer program resources

The vendor's proposed platform must be flexible enough to accommodate content sections, workflows, and user permission structures for each of these stakeholder groups. The vendor's implementation approach should include a structured stakeholder discovery process as part of project initiation, with adequate time allocated before design or development begins to capture divisional needs.

The vendor shall describe in their proposal how they approach multi-stakeholder requirements gathering for government platform projects, how conflicting priorities between divisions are resolved, and how the content management system will be structured to allow each division to manage its own content independently without affecting other sections of the site.

4.2 Outdoor Burning Eligibility Tool

The website shall include a public-facing, address-based outdoor burning eligibility tool that:

- Accepts a resident's street address

- Determines if the address is inside Fire District 4's jurisdiction
- Checks Urban Growth Area status
- Checks city limits
- Checks zoning context where available
- Applies current applicable burn ban restrictions automatically
- Applies Washington Department of Natural Resources wildfire protection area restrictions
- Routes agricultural burning inquiries to the Washington Department of Ecology
- Displays a clear, plain-language eligibility result to the resident

The tool shall produce results in categories including but not limited to:

- Residential burning allowed
- Residential burning is not allowed
- Recreational fires only
- Agricultural burning requires a state permit
- All outdoor burning is prohibited today

4.3 GIS Integration

The vendor shall handle all GIS integration required for the burning eligibility tool, including:

- Parcel layer integration
- Urban Growth Area boundaries
- Zoning boundaries
- City limits boundaries
- Fire district boundary
- DNR wildfire protection boundary
- County burn restriction status sources
- Water District's (hydrant layers, mains etc)
- Census Tracts
- Voting Precincts

Live GIS service connections are preferred over static files. The vendor shall describe their approach to maintaining current boundary and restriction data. The vendor shall also confirm that all data layers used are either publicly licensed, licensed to the vendor, or licensed at the vendor's cost, and shall indemnify the District against any data licensing claims.

4.4 Automation

The homepage shall automatically display the current burn restriction status. The system shall update restriction messaging without requiring staff to manually edit the website when county or state restrictions change. Staff shall retain a manual override option for situations such as a locally declared burn ban. The platform should also support opt-in group notifications for residents who choose to receive alerts. Notification categories should be configurable and may include fire restrictions, severe weather, traffic or access impacts, emergency notices, and other District or regional public-safety

information. Vendors shall describe supported delivery methods, subscription management, and integration with existing county notification systems.

4.5 Content Management

The District has limited administrative staff. The vendor's platform shall allow non-technical staff to update website content, including text, contact information, service hours, and public notices, without requiring training on a traditional content management system backend or knowledge of HTML.

The vendor shall describe how staff will make routine updates to the site and what level of training or ongoing vendor involvement is required.

4.6 Internal Employee Resources and Communication

The District is interested in platform support for internal employee-facing functionality. This may include access to internal resources, policies, and operational documents; employee forms and submissions; internal announcements; and intranet-style functionality for District personnel.

The vendor shall describe what internal communication and resource management capabilities are available within the platform, how access controls and permissions are managed for internal versus public-facing content, and how the internal functionality integrates with the public-facing website.

The platform shall support role-based external access for authorized third-party vendors such as the District's IT contractor, with appropriate permission controls and audit logging.

4.7 Online Payment Capabilities

The platform should support secure online payment functionality for District services. Potential use cases include burn permits, inspection fees, public records request fees, and other future District services.

The vendor shall describe supported payment processors, transaction security measures, compliance with applicable payment card industry standards, administrative workflow integration, transaction tracking and reconciliation support, and any related fees or limitations.

The Fire District procures and maintains the merchant account and payment processor. Vendor scope is integration with the District-designed processor and reconciliation tooling. Vendor shall not collect, store, or transmit payment card data. This keeps the District at SAQ-A compliance.

4.8 Emergency Alert and County Notification Integration

The District does not operate its own mass notification system. Emergency alerts and public notifications for Snohomish County are managed through SnoCoAlerts, the county-wide Emergency Notification System operated by Snohomish County Emergency Management and powered by Smart911. The District participates in this system as one of the 43 agencies served by Snohomish County 911 (SNO911).

The website shall include a prominent, clearly labeled link for residents to sign up for SnoCoAlerts and create a Smart911 Safety Profile. The vendor shall describe how the platform can display active SnoCoAlerts or county emergency notifications on the District homepage automatically, without requiring staff to manually post alert content during an active incident. The District currently uses First Arriving software for internal station-facing alerts and information dissemination. The vendor shall describe whether the platform can receive or display a feed from First Arriving for operational status displays, and shall clarify what, if any, public-facing information would be appropriate to surface on the website.

4.9 Real-Time Incident Information

Snohomish County already participates in PulsePoint, the 911-connected public safety app, through Snohomish County 911. PulsePoint connects directly to SNO911's CAD system rather than to individual agency CAD systems, which means the District does not need its own CAD integration to participate. The District is interested in exploring a PulsePoint embed or link on its website to provide residents with public-facing incident awareness.

4.10 Community Risk Reduction Program Scheduling and Registration

The Community Risk Reduction section shall support online self-service scheduling and registration for District programs and services. The District does not currently offer all of the programs listed below and expects to activate these features incrementally as capacity allows. The platform shall therefore allow individual program registration and scheduling features to be toggled on or off by staff independently, without taking the entire CRR section offline or requiring vendor involvement. At minimum, the platform shall be capable of supporting:

- Request a free home fire safety visit or smoke detector inspection
- Register for upcoming ACT+ classes offered by or through the District, or request a class for your business or large group.
- Request fire safety presentations, station tours, or other community education events
- Access seasonal preparedness resources including wildfire defensible space guidance, evacuation zone information, and emergency kit checklists

The vendor shall describe how program registrations are routed to District staff, how confirmation and reminder notifications are sent to registrants, and how registration data is retained consistent with Washington State records retention requirements.

4.11 PulsePoint and AED Registry Integration

The District is interested in integration with PulsePoint Respond and the PulsePoint AED registry. PulsePoint is a 911-connected application that alerts CPR-trained bystanders to nearby cardiac arrest events and provides a publicly accessible registry of AED locations. Integration with PulsePoint is available to public safety agencies at no cost through the PulsePoint Foundation.

The vendor shall describe whether the platform supports embedding or linking to PulsePoint community tools, and shall describe any technical requirements for connecting the website to the PulsePoint AED registry for the District's service area.

4.12 Audience-Segmented Safety Content and Multilingual Access

The website shall organize public safety content by resident audience to improve accessibility and usability. Content sections should address the distinct needs of homeowners, businesses, schools, seniors, and families with young children.

The vendor shall describe how the platform supports this content architecture and how staff can maintain audience-specific pages without technical assistance.

The platform shall support multilingual content delivery. Snohomish County has Spanish-speaking and other non-English-speaking resident populations. The vendor shall describe available translation or

language access tools, whether automated translation is supported, and how the District can ensure accuracy of translated safety-critical content.

4.13 Smart911 and Household Safety Profile Integration

Snohomish County 911 already operates Smart911, a county-wide household safety profile system that allows residents to voluntarily create a profile containing medical conditions, disabilities, household members, pets, access codes, and other information relevant to emergency response. When a registered phone number calls 911, that profile surfaces automatically on the dispatcher's screen and is relayed to responding crews. Information is not stored permanently in CAD and is only made available to 911 when the registered number initiates a call. The District is one of 43 agencies served by SNO911 and benefits from this system without any separate integration.

The website shall include a clearly labeled Smart911 signup link and a brief explanation of the program for residents. The vendor shall describe how this link is presented and whether the platform can display Smart911 enrollment statistics or community preparedness metrics where available. The District is also interested in understanding whether the platform can support similar opt-in program pages for other Snohomish County preparedness programs as they become available. Like the CRR features in Section 4.10, this capability should be toggleable by staff as programs are activated or discontinued.

5. Records Management & Public Records Request System

5.1 Integration with Website

The records management system shall connect with the public-facing website so that records requests submitted through the website are received directly in the system without manual re-entry. The website should connect with:

- The AI-supported records filing system
- The human-in-the-loop public records request workflow

Future expansion may include inspection routing tools.

5.2 Intelligent Records Search and Response Drafting

The District receives public records requests under RCW 42.56 that require staff to locate potentially responsive documents, determine what is disclosable, identify applicable exemptions, and produce a written response, all within five business days. This process currently depends entirely on staff knowledge and manual review.

The vendor's system shall go beyond document search. The system shall accept a records request, identify candidate documents from the District's archive, and assist staff by analyzing candidates against applicable provisions of the Washington Public Records Act. The system shall produce a draft response that identifies responsive records, flags documents or portions that may require withholding or redaction under RCW 42.56 exemptions and cites the relevant legal basis.

The vendor shall clearly explain how these capabilities will function for legacy records that may be scanned, poorly named, inconsistently filed, missing metadata, or stored in older formats. The proposal shall identify any limitations, preparation requirements, or manual review that may apply to legacy records. Candidate identification, exemption analysis, and suggested redactions are advisory functions only. Authorized District staff must be able to add or remove candidate records, correct classifications,

revise or reject recommendations, and approve the final response before any communication or production is released.

The system shall not require staff to know the exact file name, folder location, or metadata tags in order to locate responsive records. The system shall support search across document content, not only file names or index fields.

IMPORTANT

Staff shall retain final review and approval authority over all responses. **The vendor's AI tools are advisory only.** No draft response generated by the system shall be transmitted to a requestor without staff review and explicit approval. The vendor shall warrant in its contract that the AI system is a decision-support tool and that use of the system does not expand the District's legal liability under RCW 42.56. The vendor acknowledges that all determinations regarding exemptions, withholding, redaction, and production remain solely within the discretion of the District.

5.3 Public Records Act Compliance

The vendor's system shall track the receipt date of each public records request, calculate the response deadline based on business days per RCW 42.56, and alert staff when a deadline is approaching. The system shall maintain an audit log of all actions taken on each request, suitable for producing compliance documentation if the District's response is challenged.

5.4 Records Retention Schedule Compliance

The vendor's platform shall support Washington State Archives records retention schedules applicable to fire districts. The system shall allow retention policies to be assigned to document categories, shall flag documents approaching their retention deadline for staff review, and shall support legal hold functionality to preserve records when litigation or investigation is anticipated. The vendor shall describe how their classification methodology maps to the Washington State Archives Local Government Common Records Retention Schedule (CORE) and fire district-specific schedules.

5.5 HIPAA Compliance and Sensitive Information

The vendor's platform shall support HIPAA-compliant handling, storage, access controls, and transmission of protected health information and other sensitive data where applicable. This requirement applies because the District processes records that may involve medical incidents, emergency response patient data, personnel matters, or other sensitive information subject to federal or state privacy protections.

The vendor shall describe its security controls, access restrictions, audit logging, encryption standards, and administrative safeguards related to protected information, and shall identify any certifications or third-party attestations relevant to HIPAA compliance. The system should assist authorized staff in identifying protected health information and other sensitive content that may require redaction before disclosure. Automated detection or suggested redaction must never be treated as conclusive: authorized District staff shall review and approve each final redaction and disclosure decision. The vendor shall describe the types of HIPAA-related information the system can detect, known accuracy limitations, confidence or exception indicators, correction capabilities, and how human review and approvals are documented in the audit history.

5.6 Public Records Request Fees and Payment Tracking

The public records request system shall support the District's administration of fees, deposits, and payments associated with public records requests. At minimum, the system should allow authorized staff to prepare and issue fee estimates or invoices, record deposits and payments, associate each transaction with the applicable request, and maintain an audit history of fee-related actions.

The system should support integration with the District-selected online payment processor described in Section 4.7 while also allowing staff to record payments received through other approved methods. Staff shall retain authority to review, adjust, waive, or correct fees and payment requirements in accordance with District policy and applicable law.

The vendor shall describe how payment status affects request workflows, notifications, deadlines, installments, and final production of records.

6. Records Migration

The District currently maintains records across multiple systems and locations, including shared network drives, the fire records management system (ESO), and local storage. The vendor shall migrate the District's existing digital records to the proposed hosted platform while also establishing a regular local backup process that preserves a recoverable copy of District records under District control.

Migration shall include assisted classification and indexing of ingested documents, not simply replication of the existing folder structure. The vendor's system should propose document categories and extract searchable metadata; however, the migration process must include human validation, exception handling, quality-control sampling, correction workflows, and District approval before classifications or retention assignments are treated as final. The system should categorize documents by type (for example, inspection reports, incident reports, correspondence, permits, interlocal agreements, resolutions, and board minutes) and improve findability without requiring every record to be manually re-tagged or re-filed.

The vendor shall provide a cost estimate for migration based on the District's actual records volume, including a description of the classification methodology used. The vendor shall describe their approach to a phased migration strategy that supports both legacy and active records without disrupting daily operations, their approach to integrating with the District's existing fire records management system (currently ESO) for ongoing document ingestion after migration is complete, and their approach to future compatibility with NERIS as that platform matures.

7. Accessibility

The District is subject to ADA Title II as a special district government. The Department of Justice's April 2024 final rule requires WCAG 2.1 Level AA compliance for public-facing government websites. Under the DOJ's April 2026 Interim Final Rule, the compliance deadline for special district governments is April 26, 2028. The platform shall be built to meet WCAG 2.1 Level AA standards from launch.

The vendor's platform shall include ongoing automated accessibility monitoring and reporting as part of the subscription, not a one-time compliance audit at launch. The system shall identify accessibility issues as they arise from content updates and alert staff before non-compliant content is published to the live site.

The vendor shall describe their approach to accessibility compliance, including how they will maintain continued compliance as site content changes over time.

8. Hosting, Continuity, and Maintenance

The vendor shall describe the following in their proposal:

- Hosting environment and infrastructure
- Cloud backup approach and frequency (minimum daily backups required), plus regular local backup to District-controlled physical or on-premises storage
- Update and patching process
- Security approach, including data encryption in transit and at rest, access controls, and multi-factor authentication for administrative users
- Minimum uptime commitment of 99.9% (monthly), with defined remedies, including service credits, for failure to meet this standard
- Incident response plan and breach notification process, including compliance with RCW 19.255.010 and any successor statutes or amendments

Because the District is a public safety agency that must maintain operational continuity during emergencies, the solution shall include a continuity-of-operations approach for internet outages or service disruptions. The vendor shall describe backup access methods, redundant or offline access capabilities, and any local caching or failover mechanisms that would allow District personnel to access critical records and operational information during network interruptions. Solutions that cannot address operational continuity in a public safety environment should explain their approach to this requirement.

Local backups shall be created on a regular schedule agreed upon during implementation, shall be encrypted, shall include sufficient data and documentation to support restoration, and shall be test-restored periodically. The vendor shall describe backup format, frequency, retention, transfer method, recovery procedures, and any software or licensing required for the District or a successor vendor to use the backup independently of the vendor's hosted service.

9. Data Ownership, Security, and Continuity Requirements

9.1 Data Ownership and Portability

All data submitted to, stored in, or processed by the vendor's platform, including but not limited to public records, resident submissions, District documents, GIS query logs, and system-generated records, remains the sole property of Snohomish County Fire District 4. The vendor shall have no ownership interest in, and no right to use, sell, or share, any District data.

The proposal shall explain how the District can obtain a complete export of all District data at any time and at the end of the vendor relationship. The export must use standard, non-proprietary formats and include documents, metadata, audit history, resident submissions, website content, and other District data needed for transition or recovery.

9.2 Data Security and Privacy

The proposal shall describe encryption, role-based access, multi-factor authentication, audit logging, breach detection and notification, privacy controls, and safeguards for protected or sensitive information. The selected solution must comply with applicable Washington State and federal requirements. Final legal and contractual terms will be developed by the District and its legal counsel during the award process.

9.3 Business Continuity and Vendor Independence

The proposal shall describe how the District will maintain access to its data and essential functions during internet outages, cloud service interruptions, vendor service disruptions, or transition to another provider. The response shall address local backup, restoration, data export, documentation, domain and DNS control, and other measures that reduce dependence on continued vendor operation.

9.4 Subcontractors and Third-Party Services

The vendor shall identify all subcontractors, hosted services, third-party platforms, and external data sources that are material to the proposed solution. The prime vendor shall remain responsible for coordination and performance of the complete solution.

10. Proposal Requirements

Each proposal shall include the following:

1. Vendor overview, including organization history, size, operating experience, and evidence of financial and organizational stability
2. Evidence of relevant experience and capability, which may include references from public-sector clients, private-sector deployments of comparable complexity, or other demonstrations of the vendor's ability to deliver integrated platform solutions at the scale and operational requirements described in this RFP. The District welcomes proposals from vendors entering the public safety market and will evaluate experience holistically.
3. Proposed architecture approach, including technology stack and hosting environment. Plain-language solution overview explaining how the proposed components work together to satisfy the District's core objectives, including assumptions, exclusions, recommended phasing, and the vendor's post-selection discovery process
4. GIS integration plan for the outdoor burning eligibility tool, including data sources, licensing, and update methodology
5. Burn eligibility workflow concept, including how the system will determine eligibility across overlapping jurisdictions
6. Records management and public records approach, including how the system will assist staff while preserving human review and approval for classification, filing, retention, responsive-record selection, exemption analysis, redaction, and final response drafting under RCW 42.56
7. Records retention schedule compliance approach, including mapping to Washington State Archives CORE schedule
8. Records migration plan, including classification methodology, treatment of legacy records, human validation and quality control, estimated timeline, and cost based on the District's records volume
9. Content management approach, describing how non-technical staff will make routine updates
10. Multi-stakeholder requirements and discovery approach, describing how the vendor will gather, prioritize, and incorporate input from all District divisions during the design phase, and how the platform will support independent content management by multiple divisions (Section 4.1.1)
11. Emergency alert and county notification integration approach, including how the platform will display SnoCoAlerts and link residents to Smart911 enrollment (Section 4.8)

12. Community Risk Reduction scheduling and registration capability, including online program registration, confirmation workflows, toggleable feature activation, and data retention approach (Section 4.10)
13. Multilingual and audience-segmented content approach, including available translation tools and content architecture for distinct resident audiences (Section 4.12)
14. Accessibility compliance plan, including ongoing monitoring approach and process for preventing non-compliant content publication (Section 7)
15. Data ownership and portability approach, including export formats and timelines (Section 9.1)
16. Data security and privacy approach, including encryption standards, access controls, audit logging, sensitive-information safeguards, and breach notification procedures (Section 9.2)
17. Business continuity and vendor-independence approach, including local backup, restoration, data export, offline or alternate access, domain ownership, and transition support (Section 9.3)
18. Subcontractor and third-party service disclosure, including roles, data access, and prime vendor accountability (Sections 3 and 9.4)
19. Implementation timeline with key milestones
20. All-inclusive pricing, broken out by: setup and implementation, annual platform subscription, records migration, local backup implementation and ongoing costs, optional services, and estimated 3-year and 5-year total cost of ownership. The proposal shall clearly identify any usage limits, storage thresholds, third-party fees, or future costs.

11. Evaluation Criteria

Proposals will be evaluated based on the following criteria:

Evaluation will emphasize how clearly and credibly the proposal explains a coordinated solution to the District's core objectives. The District will not penalize a vendor for reserving detailed workflow and configuration decisions for the post-selection discovery process, provided material assumptions, limitations, dependencies, and costs are clearly disclosed.

Criterion	Weight
Technical capability and platform delivery — including records management, PRR system, GIS and burning eligibility tool, public-facing website, records migration, and platform integration	50%
Data protection, legal provisions, and compliance — including data ownership, security, breach notification, business continuity, and accessibility	25%
Vendor qualifications and implementation — including relevant experience, financial stability, and implementation timeline	15%
Total cost of ownership (3-year)	10%

The District is not obligated to select the lowest-cost proposal. The District reserves the right to conduct interviews, request clarifications, or request best-and-final offers from finalists before making an award decision.

12. RFP Terms and Conditions

District shall not be responsible for any costs incurred by the Vendor in preparing, submitting or presenting its response to the RFP.

All received proposals are subject to the Washington State Public Records Act, Chapter 42.56 RCW. Any information in the Proposal that the Proposer desires to claim as proprietary and thus exempt from disclosure under the provisions of existing state law, shall be clearly designated. Each page claimed to be exempt from disclosure must be clearly identified by the word “Confidential” printed on it. Marking the entire Proposal exempt from disclosure will not be honored. If the District receives a public record request for any information that the Proposer has designated as proprietary, the District’s sole obligation will be to notify the Proposer that a request has been received and that the District will release such information within ten business days of notifying the Proposer unless Proposer obtains a court order enjoining disclosure under RCW 42.56.540.

The successful Vendor must comply with Washington State equal opportunity requirements. District is committed to a program of equal employment opportunity regardless of race, color, creed, sex, age, nationality or disability.

The selected Vendor shall maintain insurance that is sufficient to protect the Vendor’s business against all applicable risks in a manner acceptable to District.

As a result of the selection of a vendor to supply the Equipment to District, the Vendor agrees to make no reference to District in any literature, promotional material, brochures, sales presentation or the like without the express written consent of District.

Submittal and signature of a proposal swears that the document is genuine and not a sham or collusive and not made in the interest of any person not named, and that the Vendor has not induced or solicited others to submit a sham offer, or to refrain from proposing.

Selected vendor will be expected to enter into a contract with terms developed by the District and its legal counsel during the award process.

13. Submission Instructions

Proposals shall be submitted electronically to:

DJ Hill, Fire Marshal

Snohomish County Fire District 4

Djh@snohomishfire.org

Proposals are due by September 25, 2026 at 5:00 PM Pacific Time. Late submissions will not be considered.

Questions regarding this RFP must be submitted in writing to the Fire Marshal at the contact information above no later than September 1, 2026. All questions and answers will be shared with all prospective vendors via written addendum. No oral interpretations will be made.

Schedule of Events

<u>Milestone</u>	<u>Date</u>
RFP Issued	August 14 th , 2026
Questions Due	September 1, 2026
Responses to Questions Issued	September 11 th , 2026
Proposal Due Date	September 25, 2026
Proposals Scored	September 29, 2026
Consultant Interviews (if required)	October 7-9, 2026
Selection and Notice of Award	October 12, 2026
Contract Execution	October 13 to 23, 2026
Project Commencement	November 1, 2026