Kitsap County
Financial Management System Replacement

Phase 1: HRIS & Payroll

2018-139

TABLE OF CONTENTS

Request for Information Overview 2018-139

Kitsap County AUDITOR'S OFFICE AND DEPARTMENT OF HUMAN RESOURCES
NOTICE TO CONSULTANTS FOR CONTRACT MANAGEMENT SOFTWARE

RESPONSE DEADLINE: Tuesday, July 31, 2018 @ 3:00 p.m.

Kitsap County Auditor's Office and Department of Human Resources is soliciting information from qualified vendors relating to the replacement of the County 's financial management systems to be implemented in phases with priority given to Payroll and Human Resource functions. The solution may be a single, all-inclusive solution with implementation in phases or separate modules that connect efficiently with other modules and existing technology.

The purpose of this Request for Information (RFI) is to gather information regarding possible solutions that address the needs discussed within this RFI. This is not a solicitation to purchase services and/or goods. No contract will be awarded based on the responses to this RFI. However, depending upon knowledge gained from the response to this RFI, it is Kitsap County 's intent to take the next steps required for procurement of technology or services.

This RFI is designed to provide vendors with the information necessary for the preparation of informative responses. This RFI process is for Kitsap County 's benefit and is intended to provide information to facilitate the future selection of goods and services. The RFI is not intended to be comprehensive and each vendor is responsible for determining detail of response. Vendors may be requested to demonstrate their product at a Kitsap County facility.

Kitsap County assumes no financial responsibility in connection with the vendors' costs incurred in the preparation and submission of the RFI packets, nor shall it constitute a commitment, in any way. Kitsap County reserves the right to cancel this RFI if it is deemed in the best interest of the County to do so.

Kitsap County will treat all information submitted by a vendor as public information unless the vendor properly requests that the information be treated as confidential at the time of submitting the response. Any requests for confidential treatment of information must be stated within the executive summary in the vendor's RFI response. The request must also include the name, address, and telephone number of the person authorized by the vendor to respond to any inquiries concerning the confidential status of the materials. Each page shall be marked as containing confidential information and must be clearly identifiable to the reader.

Please submit one (1) original and one (1) digital copy (USB drive or CD) by **TUESDAY, JULY 31, 2018 3:00 PM. Faxes, emailed and late response will not be accepted**. Information may be delivered to the addresses below:

By Mail	**OR**	**Express, Courier, or Hand delivery**
Colby Wattling		Colby Wattling
Kitsap County Department of		Kitsap County Department of
Administrative Services		Administrative Services
Purchasing Office		Purchasing Office – Fourth Floor
614 Division Street MS-7		619 Division Street
Port Orchard, WA 98366		Port Orchard, WA 98366

Any questions regarding this RFI should be directed to Mary Collins, Enterprise Process Analyst 360-337-4662, or mlcollins@co.kitsap.wa.us

Persons with disabilities may request that this information be prepared and supplied in alternate forms by calling collect 360-337-5777 or TTY 360-337-5455.

The recipient, in accordance with Title VI of the Civil Rights Act of 1964, 78 Stat. 252, 42 U.S.C. 2000d to 2000d-4 and Title 49, Code of Federal Regulations, Department of Transportation, Subtitle A, Office of the Secretary, Part 21, Nondiscrimination in Federally-assisted programs of the Department of Transportation issued pursuant to such Act, hereby notifies all consultants that it will affirmatively ensure that in any contract entered into pursuant to this advertisement, disadvantaged business enterprises as defined at 49 CFR Part 23 will be afforded full opportunity to submit qualifications in response to this invitation and will not be discriminated against on the grounds of race, color, national origin, or sex in consideration for an award.

Project Overview

About Kitsap County

Kitsap County (the 7th largest in Washington State) serves an amazing community of more than 260,000 residents. The County 's Auditor and Human Resources Departments provides essential functions to the county, such as labor relations, payroll services, public accountability, providing a great working environment for 1,200 full-time and 600 part-time employees. During the past 24 years the Auditor has made the best use of a software solution designed for manufacturing which was adopted for governmental accounting. The modifications, work-arounds, and patches have finally come to a point where the system is no longer able to function at the expected, and required, levels of performance causing mandatory overtime and unnecessary stress to staff.

We must now prepare for a successful transition from our legacy Financial Management System (FMS) to a new FMS that integrates with Human Resources and Information Systems. As we continue to support the legacy system, our workforce is taxed with many manual work-arounds, downtime, and overtime to perform key functions. Our immediate needs require a payroll and human resource management solution; however, a comprehensive ERP solution will be highly desired for our future needs.

Volume Statistics

Statistic	**Total**
Fixed Assets maintained on System	14,400
Vendor Payment Vouchers processed/year	42,604
Manual Warrants/year	28,410
Intergovernmental Vouchers processed/year	1,261*
Journal Vouchers processed/year	26,127
Current number of Funds	390
Employees Paid / Month (includes Special Purpose District)	2,192
Current Vendors	20,549
Contracts processed in 2017	1,055
Tax Parcel Numbers in 2017	124,161

** Estimated number*

Current Situation

Currently, Kitsap County uses JD Edwards for financial management and human resource management. It also combines various other applications to augment workflow such as, Kronos, Hubble, NEOGOV, Halogen, BenefitFocus and Risk RT.

The current FMS application systems are inefficient and lack the services needed. This results in manual work that increases time for processing and opportunity for errors. There is a lack of transparency in transactions and employees feel as though they are not getting reliable information.

Some examples of issues with the current solution are

- System requires rework, manual activities and work arounds
- Requires specific skill set from Information Services (IS) to manage customizations
- Required reporting is labor intensive due to there being no templated reports nor ad hoc reporting features and a very limited number of user who can create reports.
- Manual calculations needed for retro calculations and tracking protected leave
- Requires customized solutions for interfacing (cash and Hubble)

Due to the system's age there are support challenges from both the vendor and internally. Historically the cost for additional licenses has limited who can access FMS. This has resulted in workarounds and customizations to input and provide information.

The current system has many customizations that are not able to be supported either due to technical limitations or excessive resource requirements.

Being the central FMS system, it needs to interface with many other systems such as, performance management systems, reporting tools, IT user systems, recruiting apps, document recording systems, etc.

The system does not house automated equipment billing for Public Works and is not flexible enough to accommodate 13 collective bargaining agreements or Fair Labor Standards Act overtime calculations. Also, all employees are treated as hourly employees by the current solution and has limitations for making salary provisions.

The system does not interface with other systems easily. It requires proprietary Data Name Source (DNS) configurations and Data Source Types to interface with other data sources like Access, SQL Server, Visual Studio, IIS, etc.

Kitsap County also uses Vertex software, which needs frequent updates as part of national tax law changes. A technology solution must be able to accommodate this and other legal requirements.

Due to lack of data integration within the current system, position ID number status must be updated manually based on hires and terminations.

Deployed Technology

Name	Version/ Current	Hardware	Software	Strategy
JDE	A9.3.1.3/ 9.4	iSeries - currently hardware is on extended support	On perpetual support by Oracle. Includes Windows installations of Reflections, IBM Client,	Software Updates are typically installed as needed for functionality or security. Average between 4 and 6 per year.

Name	Version/ Current	Hardware	Software	Strategy
			System iNavigator, Access, etc.	Version updates may happen every 2 or 3 years as needed for Software Update requirements.
Halogen	17.1.4.21/ 17.2	KCAPP5 – Windows Server 2012 R2	On yearly support by Halogen	Version updates are requested by end users. Upgrades are a coordinated effort by IS staff and vendor.
Kronos	7.0.3/8.0	iSeries - currently hardware is on extended support	On perpetual support by Kronos. Includes JD Edwards interface and Web interface.	Version update was requested by Payroll but is postponed due to this project.
Benefit Focus	2018(Vendor Supported)	Cloud solution	Web	Currently a manual process.
Hubble	2016.1 SP3 (latest)	iSeries - currently hardware is on extended support	On perpetual support by Hubble. Includes JD Edwards components and local Windows application	Offers several other interfaces but may not be needed in the new system.
RisKRT	2018 (Vendor Supported)	Cloud solution	SaaS	Used for ACA reporting. Connect employee reporting data from HRIS Solution.
NeoGov (Insight)	2018 (Vendor Supported)	Cloud solution	SaaS	Connect recruitment and new hire information with HRIS
SharePoint	2010, 2013	Windows SharePoint servers	SharePoint, custom ASP.Net and .Net Windows application used for PDF splitters	Would like to deprecate the splitter programs
Access Databases	2016		MS Access	There are multiple access databases that are used to pull data out to for reports and other work arounds. The strategy is to remove the need for reliance on secondary systems to provide the features we need with a new FMS solution.
PayView	2010, 2017 (admin)	Intranet	ASP.Net, IIS	Used by all employees to view paystub history. Admin is used to give permissions to timekeepers.
Voucher Search	2018	SQL Server (linked tables)	ILINX	Used to pull up vouchers in PDF format. Links to JDE files for voucher and Address Book information.

Name	Version/ Current	Hardware	Software	Strategy
HR Personnel Files	2018	SQL Server (linked tables)	ILINX	Used to pull up HR Personnel files in PDF format. Links to JDE files for Address Book information.

Equipment Performance and Reliability

IBM iSeries –

- Uptime: down daily from 1am to 4am
- H/W Patching frequency: as needed 2-3 years
- D/R plan: failover at remote site with secondary equipment
- Age of equipment (Risk): 2005
- Backup/Recovery: nightly full tape backup

Current Issues/Reasons for Change

There are two primary reasons driving change:

1) The IBM iSeries server which runs our current system is reaching end of life. It will be up to Information Services (IS) to find a solution that will take us into 2019 as we continue the migration to a new FMS. There are three options that are being evaluated: a) Find a third-party to take over hardware maintenance; b) Piece together a new server to transfer the system; c) Move the existing software up to a cloud host.

2) The current FMS solution was deployed 24 years ago and over time the system's functionality has not been able to scale with the legal requirements, labor relations, and interoperability with other reporting software. During this transition, we will explore Software as a Service and on-premise options from individual vendors and multiple vendors that can provide interoperability for our system requirements.

Incumbent Providers (To Be Replaced or Must Have Efficient Connection To)

Secondary system that are being evaluated for replacement are:

- Halogen – Performance Management and LMS – On Premise
- Kronos – Time Keeping (on site, same Server challenge)
- Neogov - Recruitment
- Hubble – Reporting for JDE (on site, same Server challenge)
- BenefitFocus – Benefits Enrollment and Tracking (currently manual entry)
- Risk RT – Affordable Care Act Tracking

Relationship Between Incumbent and Selected Provider

On premise - The current financial system is vendor supported. The County has a direct relationship with vendor resources. Break/fix and enhancement issues are escalated within the County by lines of business and internal IT. Solutions are deployed and tested using vendor and County resources.

Specific Issues/Concerns

The current FMS solution does not interface with most of Kitsap County 's secondary systems, thus requiring manual data entry of data by staff into those secondary system. The current system is unable to integrate software updates, causing application failures during required patches. This requires users and IS staff to rebuild all customizations.

Commonly expressed concerns include:

- System requires rework, manual activities and work arounds
- Requires specific skill set from IS to manage customizations
- Requires frequent vendor support
- Required reporting is labor intensive due to there being no templated reports nor ad hoc reporting features and a very limited number of user who can create reports.
- Manual calculations needed for retro calculations and tracking protected leave
- Requires customized solutions for interfacing (e.g. Cash and Hubble)
- Manual entry for Open Enrollment (e.g. BenefitFocus)

Incumbent Providers (To Remain in Place)

If Kitsap County chooses not to replace secondary systems listed above, integration between the new solution and secondary systems/providers is desired. Furthermore, the new solution's future upgrades should not affect integration between listed secondary systems.

Secondary system that need to be able to integrate are:

- Halogen – Performance Management and LMS – On Premise
- Kronos – Time Keeping
- Neogov - Recruitment
- Hubble – Reporting
- BenefitFocus – Benefits Enrollment and Tracking
- Risk RT – Affordable Care Act Tracking

Relationship Between Incumbent and Selected Provider

On premise - The current financial system is vendor supported. The County has a direct relationship with vendor resources. Break/fix and enhancement issues are escalated within the County by lines of business and internal IT. Solutions are deployed and tested using vendor and County resources.

The selected provider must be able to demonstrate the efficacy of proposed solutions. They must work with the County as a partner to ensure success. Communications should occur through appropriate channels based on mutually agreed upon roles and responsibilities. The provider must have an existing process for acquiring customer suggested enhancements and their subsequent incorporation and deployment through planned updates.

Specific Issues/Concerns

- The solution should replace current secondary processes for tracking various leave accrual rules, FLSA overtime calculations, payroll deductions, etc.….
- All changes must have an audit log and be able to be identified by end users

- Support multiple employee types based on 13 separate unions and multiple separately elected offices, and widely varying employee types (e.g. general administration, patrol officers, medical personnel, road crew, engineers, legal professionals, field inspectors, elected officials, judges).
- Provide employee portal without secondary systems to support such activity as viewing paystubs and W2s.
- Compatible with KeyBank's eft payment system and facilitate file transfers.
- Payroll, Timekeepers, HR, and Treasurers sometimes lock files that are being used by somebody else causing jobs to hang up and often require IS resources to review job logs.

Ongoing Activities That May Affect This Project

Kitsap County has several ongoing activities that may affect this project:

- Implement Union Contract Changes
  (annually, November - December)
- Open Enrollment
  (annually, November – December)
- 13th Month end of year reconciliation (W-2 and 1099)
  (annually, January)
- Budget Hearings (annually, September)
- Tax Collection (bi-annually late April, late October)

Desired State

Kitsap County requires an FMS solution that meets the items reflected in Appendix 3 – Solution Requirements). We require the vendor to provide Federal and State regulated updates in accordance with the law. We require our vendor to help us reduce total cost of support requirements by providing tiered service-level agreements for the next several years. We need a solution partner who will also help us capture value from our current processes and guide us through real-world problems with their solution. We are looking for a vendor to provide prevention-based approaches that deliver more value to our work. Preferred state is an entire out of the box system to implement stage by stage and perform all financial tasks within the county OR a limited number of separate software that will integrate to provide seamless workflows between departments. The system should be configured to work with the Treasurer's office to clear transactions in preparation for the monthly reconciliation process. The system should be compatible with KeyBank's eft payment system and facilitate file transfers.

Planned/Anticipated Deployed Technology

Kitsap County preferably seeks a SaaS solution with available APIs that allows interoperability between multiple systems, including the legacy system, JD Edwards. Although a SaaS system is not our exclusive choice, it is initially the preferred choice to keep maintenance costs lower than a dedicated on-premise hardware and software solution. The county would like a single ERP solution yet understands that it may be better for the county to work with multiple vendors in pursuing our objectives to leave our legacy system for a modern system that will take us into the future.

The intended solution and associated interconnections with secondary systems should require support at current resource levels (or less) and capitalize on existing resource capability. For example, the dominant county architecture on premise involves running Microsoft services on a VMware cluster. Any on-premise

solution should be compatible with both Microsoft services and the interconnections with the secondary systems.

Nature of Service Required

The proposed solution service level objectives should meet the following requirements:

Intent: To promote a proactive, responsive relationship with the incumbent to ensure continuity of operations, customer privacy and security, optimize system health, increase system uptime with a high level of customer satisfaction.

Scope: Includes all customer service request activity including but not limited to reactive (break/fix) responses, proactive preventative maintenance activity, application patching and upgrades, system monitoring and alerts, and service request activity tracking via email, customer portal, phone or otherwise. Also includes the timing, scheduling and deployment of solutions in terms of priority and impact to operations as defined by the incumbent's service schedules.

Availability: For SaaS solutions a monthly uptime percentage of 99.95% is desired. This is calculated by subtracting from 100% the percentage of minutes during the month in which the software application is unavailable (Excluding downtime resulting directly or indirectly from any SLA Exclusion). In addition, overall SaaS SLA performance metrics should be monitored and readily available to the County. At a minimum these metrics should include service availability, applied security measures and defect rates. For SaaS and on-premise solutions provider support must be accessible during the County's normal business hours Mon-Fri 8am-5pm PST. The provider's problem resolution response should include a prioritized ticketing system that is accessible via phone, web customer portal and email. Solution provider responses to prioritized support tickets should meet or exceed the following response times.

Critical Work stoppage – 2 hours

High - same day

Normal - 48 hours

Low – 7 days

In all cases an automated response does NOT constitute a sufficient response when computing response time. In addition, the solution provider must be able to provide a backup copy of the customer data (in .bak) format either quarterly and/or upon request.

Security: Must meet all requirements in Appendix 4 – Kitsap County Information Services Security Policy and Appendix 5 - Kitsap County Security Questionnaire

Privacy: Compliance with all HIPAA and EPHI data protocols and regulations, including but not limited to audit logs specific to HIPAA and EPHI controls

Disaster Recovery: Data recovery time objective immediate to 24 hours

Records retention: Ability to meet varying records retention requirements from none to permanent and be agile enough to keep up with retention changes.

Remediation: Issuance of service credits must not be the sole remedy where solution does not meet SLA. The solution provider should provide a cure for any such breach within 30 days of discovery. The customer reserves the right to terminate the service based on the number of breaches i.e. performance.

Transition Requirements

The FMS transition team estimates 6 months of running the old system and new system in parallel. After it has been proven that all data integrity is as expected we would retire relevant modules on the previous system. Prior to this, we will need the ability to populate the new system with data dating back to 1/1/2019 to facilitate end of year reporting. We will need a way to populate the uninvolved modules of our current FMS solution, specifically the General Ledger facilitate the reporting requirements set out as part of the comprehensive annual financial report. Since the county's budget approval cycle is yearly we will need to establish a contractual agreement that ensures a complete installation and migration for Payroll and HRIS during 2019 and a projection of costs for up to 5 years. Training materials and resources for payroll, timekeeping and human resources personnel are required.

Acceptable Levels of Disruption

Training and learning curves for the new system are to be expected during the first 90 days from "go live". We have been operating from a break/fix reactive mode and understand that transitioning to a proactive mode will require additional time initially, but we clearly expect to see efficiency gains that will free workload from IS, Human Resources (HR), and Payroll. We understand that additional disruption may also come from data gathering between old processes and new processes during this transition. We expect workload and overtime may not significantly reduce in the first 90 days, however, we do expect to see significant reductions overtime for payroll within 9 – 12 months.

Transition-Related Costs

Transition costs include technical assessment of environment to determine optimal maintenance plan, acquisition of additional hardware/software resources to accommodate or support solution and its connectivity to remaining incumbent providers, also start up training costs associated using both legacy and new solutions simultaneously during transition. Additional data migration costs may be included in the overall project.

Data Migration Concerns

Kitsap County may need to access historical HR and Payroll data generated prior to implementation and needs to be able to address how much historical data to migrate from our current system to lessen the need to access unmigrated data. We also may need to identify where to store unmigrated data for future reference purposes.

Level of Involvement from Kitsap County

Kitsap County will provide a project manager and SME leads during all phases of implementation, including IT resources. Potential vendors should include an additionally expected involvement from Kitsap County for a successful implementation of their solution.

Objectives of Change

Kitsap County 's primary objective to move to a new solution is to increase efficiency of our processes by reducing customizations and reliance on secondary systems and increase quality by reducing the opportunity for errors resulting and increased confidence in system stability. We expect to see a reduction in overtime required to process payroll. We intend to have many manual tasks automated to reduce the workload currently required in supporting our legacy system.

Financial Benefits

The county will directly save hundreds of hours of overtime per year in calculating payroll. The new system will also provide unprecedented synergy between HR and Payroll which will equate to measurable

dollar savings over three years. After the initial testing phase of the new system we anticipate overtime from Payroll to drop significantly.

Portfolio Performance Improvements

As previously mentioned the existing on-premise FMS solution has dependencies on end-of-lifecycle technologies requiring specialized support knowledge and expertise. Expected portfolio improvements due to usage of current technologies include expanded qualified labor pool, less down-time due to scheduled and un-scheduled maintenance (improved system stability and availability) and a reduction in the number of break-fix activities due to customization.

Service Improvements

The current solution service metrics includes both in-house and vendor ticket response metrics. In general, in-house responses are same day for break/fix and 10 days for proactive service requests. Vendor response levels as indicated in SLA sections of this document. Support ticket volume averages about 60/yr. break/fix and 60/yr. service requests. The County's expectation is that the solution provider would improve upon these metrics.

Success Criteria

The ERP will be considered successful when we implement an ERP system meeting the requirements in Appendix 3 within two to four phases that last no more than two years. The first phase will be a system that provides all critical functions of the County 's Payroll function and Human Resources Information System (HRIS). This first phase will alleviate the pain experienced by Payroll from using the legacy system. The new system will be able to handle the needs of HR and labor negotiations with up to 13 contracts without requiring manual calculations. System will also have the ability to integrate employee management functions such as Recruiting, Onboarding, Performance Reviews, Case Management, Learning Management, and other Human Resources functions. The system will successfully run in parallel to the legacy system for 6 months to gather enough data for two full backfill cycles and be able to seamlessly connect to the legacy system as the County implements remaining phases. Success will also be gauged by the level of value the vendor can add to Kitsap County 's Payroll and HR processes. We will reduce JD Edwards related overtime hours by 75%.

Service Schedule Definition

Reactive Break/Fix Requirements

In any type of break/fix for the on premises hardware, we need to have initiation and diagnostic inspection of the hardware on a same-day basis. Payroll weeks are typically scheduled out to the hour, so we need to have a handle on work stoppage for Payroll processes. Oracle support for JDE offers different levels such as Critical, Significant, Standard, and Minimal.

Solution provider responses to prioritized reactive support tickets should meet or exceed the following response times including estimate of time to return to service:

Critical Work stoppage – 2 hours

High - same day

Normal - 48 hours

Low – 7 days

Similar capability to (or compatibility with) Microsoft System Center Operations Manager. Monitored events should indicate application health, server resource allocation and utilization. Alerts should indicate

disk space and CPU utilization, whether application critical services are stopped and/or if IIS applications are no longer available. Notification of outage and estimate of time to return to service.

Proactive/Preventive Maintenance Requirements

Proactive remote monitoring should include similar capability to (or compatibility with) Microsoft System Center Operations Manager. Monitored events should indicate application health, server resource allocation and utilization. A baseline performance assessment will be provided so that future performance bottlenecks can be quickly identified. Alerts should indicate the following, policy updates, patching and conditions where additional maintenance is required i.e. deviation from baseline performance. 30-day notification of scheduled maintenance outages and estimate of time to return to service. For SaaS solutions County data must be available for download (either on request or scheduled) for internal review and development. Database backups via Sftp or other secure method is preferable.

Value-Added Services

Service elements within this category may include:

- Basic input/output system (BIOS)/firmware update application
- Operating system support
- Hardware inventory management/true-ups
- Equipment disposal
- Warranty management
- Lease management

Defined Service Schedules

Communication regarding service schedules is required 10 days prior to scheduled maintenance activity. Any unscheduled maintenance must be communicated and coordinated with designated County contact personnel.

Table 1. Example of a Service Schedule

Service Activity	Schedule
Break/Fix	Real-time
Performance Monitoring	Real-time
OS/Hardware Support	Real-time
OS Security Patching	Monthly
Application Patching	Quarterly

Pricing

Pricing Structure

Must include all costs associated with implementation; including consulting, hardware, software, travel, etc. All annual costs with an assumption of one-year subscription with 3 renewals. For the below number of users and roles listed in Table 4 Roles and Users, annual miniatous costs, costs for customizations, support costs, and any other costs that would be incurred during the life of a contract.

Table 2 Roles and Users

This assumes that employee self-service users would not need a license.

Role	Number of Users – Phase 1 Payroll and HRIS	Number of Users – Phase 2 The rest of FMS
IT Admin (System engineer and/or Programmer)	10	6
Super User (User Admin.)	10	10
Edit and Contribute Users	60	90
Read Only Users	15	25

Additional Requirements

Reporting

Reporting features need to be able to address the areas:

- Key performance indicators
  - Mean Time Between Failures (MTBF)
  - Mean time to resolution (Mean Time to Repair (MTTR))
  - Levels of responsiveness
  - Equipment availability
  - SLA compliance
  - Repeat incident frequency
- Operational metrics
  - Details of replacement part usage
  - Capacity vs. utilization ratio
  - Operational risk profile
  - Spares inventory costs and levels
- Level of report detail required
  - Equal Employment Opportunity Plan (EEOP) reporting
  - Equal Employment Opportunity Commission (EEO-4) reporting
  - Affordable Care Act (ACA) reporting
  - Costing and Workforce Analysis
  - Benefit census
  - Historical Data
- Frequency of reporting
  - Scheduled
  - On Demand
- Format of reports
  - Excel
  - Word
  - PDF
  - CSV
  - SQL if applicable
- Availability of data online (Ad Hoc)
  - Interface to view personal information by user
  - Interface for Special Purpose Districts to view payroll data

Review Meetings

Regular project and solution support review meetings will be identified within the contract.

Service-Level Requirements

Kitsap County is intent on ensuring that the level of service delivered by its selected provider consistently meets its stated operational requirements. To this end, Kitsap County would like to establish a set of SLAs underpinned by a penalty-and-reward structure that encourages consistent delivery and rewards service provider performance that materially benefits Kitsap County.

Key Performance Indicators/Primary Metrics

Kitsap County will establish a series of key performance indicators related to the consolidated hardware maintenance contract. The number and nature of these metrics has not yet been fully defined and Kitsap County is keen for prospective providers to work with us to determine the optimum number of measures that give sufficient visibility of overall service delivery performance without incurring additional unnecessary administration burden.
Key performance indicators for this consolidated hardware maintenance contract may include, but may not be limited to, the following:

- Data accuracy
- System functionality as promised
- Processes take less time to complete
- Mean Time Between Failures (MTBF)
- Mean Time to Repair (MTTR)
- Levels of responsiveness
- Equipment availability
- SLA compliance
- Repeat incident frequency

Ongoing Management of the Agreement

Contract Duration

Kitsap County welcomes proposals based upon the following contract durations:

- One year
- Two years
- Three years

Access to Service Data (Inventory, Equipment Incident Histories, Parts Usage Statistics Warranty Claims, and So Forth)

Kitsap County recognizes that as part of its delivery of these services the selected service provider will collect and retain significant volumes of data relating to KITSAP COUNTY's infrastructure that would be beneficial to Kitsap County if it determined it wished to switch providers. Please confirm that the ownership of all such data remains with Kitsap County and describe the process to return this data and the format that said data will be delivered via in the event of such a situation.

Capability Demonstration

Comparable Industry and Technology

Vendors should have experience with customers in mid-size County or Cities, preferably in the State of Washington. These customers should have similar structure and needs (e.g. unions, multiple retirement systems, etc.). Exceptions to this will be considered only for pilots and will require the agreement from the IS Steering Committee. For SaaS solutions we will consider deploying where the release level has been generally available for at least six months and has similar customers in production.

Preventive Maintenance Competence

The vendor solution needs to provide flexible upgrade and patching plans that work around annual workloads and changes in regulations.

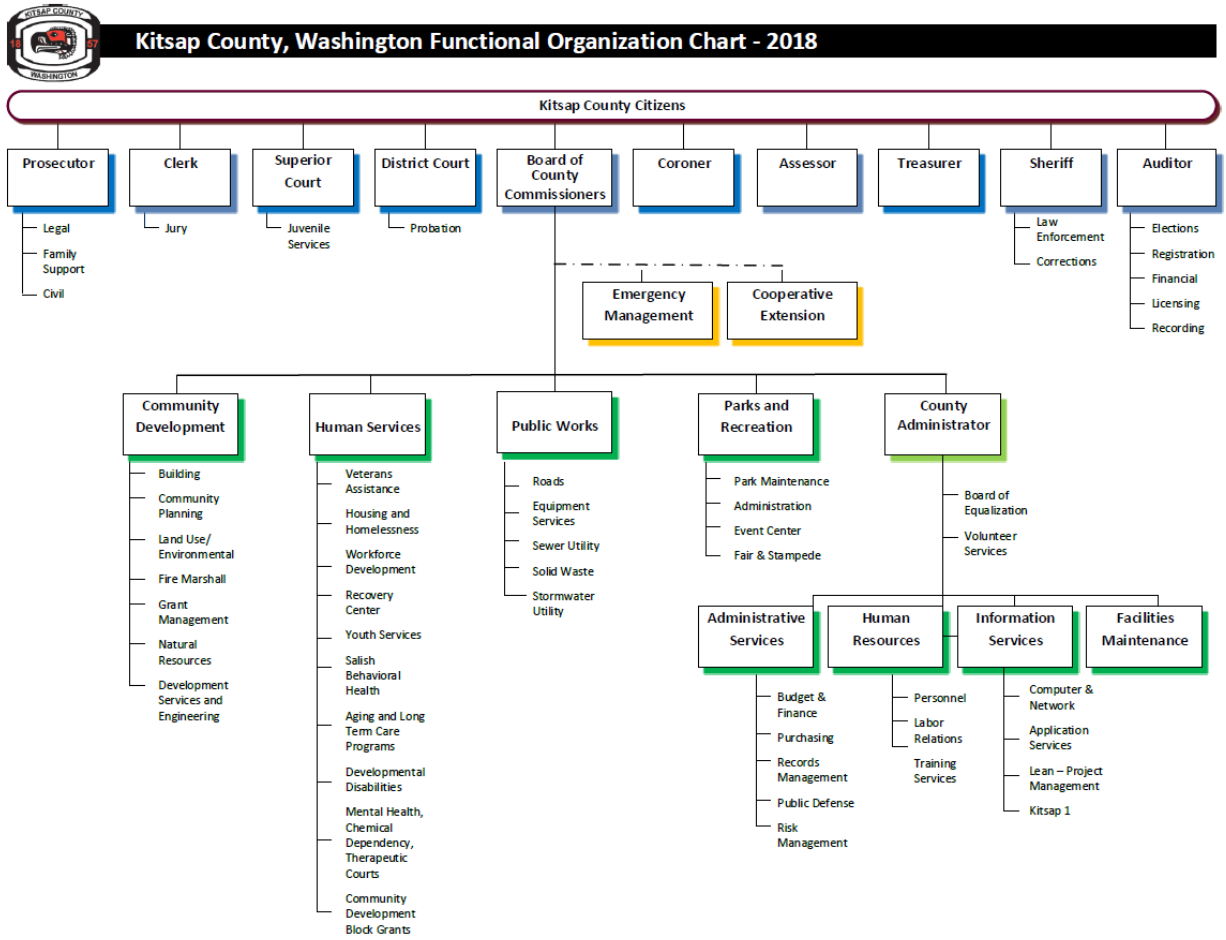
Technical Skills and Proficiency

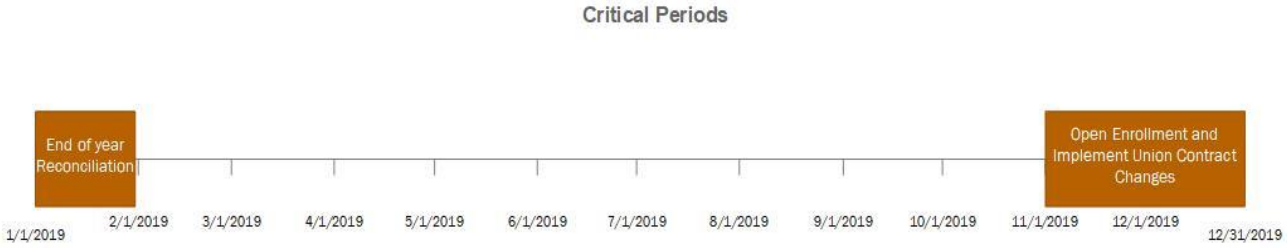
Potential solutions will provide a testing and training environment. They will have a clear escalation path for issues, mitigation, and resolutions for support that goes beyond basic technical support.

Customer References

Please provide details of three customer references with contact information to whom you are providing consolidated maintenance services that you consider relevant to our situation. References should be chosen for the similarity of their business requirements and needs, and for the similarity of their platform requirements. For each reference, please indicate your reasoning for selecting them and how you believe their circumstances are comparable to our own.

Appendix 1 — Organizational Structure and Peak Usage/Operationally Critical Periods





Appendix 2 — Specific Features Questionnaire

Vendors must specifically respond to each of the following questions

Placing a "Y" in the Out of the Box column indicates that the functions are contained in the solution proposed. Placing a "Y" in the Custom column indicates that a custom modification will be required. Please provide specific answers to questions in the response cells and if needed on a separate document. Reference the question number from the table below.				
1	**Feature**	**Description and/or Clarification**	**Out of the Box**	**Custom**
			Response	
1 Functionality				
1.1	Admin. Users	Do you have "out of the box" role-specific user interfaces including support for end users/novices, general IT professionals/intermediate and repository administrators/advanced types of users?		
1.2	Menu Customization	Does the user interface allow for the addition of custom menus and menu items?		
1.3	Different User Group Menus	Can menus be tailored for different groups of users?		
1.4	Process Management	Other than menus, does the tool provide process management facilities to guide users through the tasks they need to perform?		
1.5	Portal	Does the user interface include a portal/internet browser capability?		
1.6	Multiple Windows	Does the user interface support multiple "windows" open at once? If so, do changes to repository artifacts result in all affected windows being refreshed at once?		
1.7	Minimal Technical Customizations	Can you provide 90% of requirement without additional customizations?		
1.8	Updates for Regulatory Changes	Are you able to adapt to frequent regulatory changes and apply Best Business practices as they are needed?		
1.9	Manage and Update Payrates	Is tool able to create pay scales without using secondary systems. For example, user should be able to select several (not all) paygrades and ask the system to automatically calculate a 1.5% increase for just the selected pay grades?		
1.10	Talks to Other Systems	Is tool able integrate with secondary systems? Can updates from secondary systems easily transfer to the tool, so new employees don't have to be manually added to secondary systems and vice versa?		
1.11	Allows updating F/T & P/T pay	Is tool able to mass update pay rates in employee records, including part time employees?		
1.12	Handles variances in process, policies, practices	Is tool able to accommodate variances based on the County 's complex Union environment? I.e. pay practices, accruals, overtime calculations, shift and differential pay, pay rates, etc.…		
1.13	Date Adjustments Made Easier	IS tool able to recognize what dates needs to be adjusted based on the event entered? For example, when someone		

Placing a "Y" in the Out of the Box column indicates that the functions are contained in the solution proposed. Placing a "Y" in the Custom column indicates that a custom modification will be required. Please provide specific answers to questions in the response cells and if needed on a separate document. Reference the question number from the table below.				
1	**Feature**	**Description and/or Clarification**	**Out of the Box**	**Custom**
			Response	
		has an employment change in status, the tool would automatically update all applicable fields with adjusted dates.		
1.14	Superuser flexibility	In the tool, are superusers able to make changes or set parameters for functions without having to contact the vendor and waiting for vendor to update? E.g. Social Security Number changes, Provider changes, etc...		
1.15	Deferred Comp	Is the solution able to accommodate changes to deferred compensation without manual processes?		
1.16	Date Configurations	Does the solution support date specific calculations such as, start date at beginning of pay period, end date at end of pay period?		
1.17	Connection to KeyBank	Can the solution create a Positive Pay file for KeyBank?		
1.18	Support Multiple Union	Is solution able to customize employee's benefits, pay, and leave accrual based on their union designation?		
1.19	Support Multiple Districts	Is solution able to have Special Purpose districts access the correct layer of information for themselves, without assistance from payroll staff?		
1.20	Run Multiple versions of Payroll	Can tool run multiple Payroll versions for the County (bi-weekly) and Special Purpose Districts (monthly)?		
2 Technology				
2.1	Operating system	Which platforms, operating systems and databases does your repository run in/support "out of the box" in your base product? Please describe components such as client/browser/portal, middleware/communication protocols, servers and database management systems separately.		
2.2	Client Access	Can the multiple clients of different types access the same server platform?		
2.3	HW Config. Requirements	What are the minimum and recommended hardware configuration requirements?		
2.4	Cloud Config.	Do you offer cloud-based configurations for your repository?		
2.5	User Interface	Is it possible to develop customized user interfaces? If "yes," what tools or services are required for customization?		
2.6	Create Views of Data Repository	Is it possible to create aggregated/scoped "views" of data in the repository based on role of user, artifact grouping (e.g., by project), or model sub-setting (e.g., only the artifacts for the accounting organization or only "production artifacts")?		
2.7	API for metadata query	Does your repository have an API for programmatic query of metadata in the repository?		
2.8	Prevent Updates	Does the repository have the ability to "freeze" a configuration to prevent undesirable updates while allowing changes to other artifacts to continue?		

Placing a "Y" in the Out of the Box column indicates that the functions are contained in the solution proposed. Placing a "Y" in the Custom column indicates that a custom modification will be required. Please provide specific answers to questions in the response cells and if needed on a separate document. Reference the question number from the table below.				
1	**Feature**	**Description and/or Clarification**	**Out of the Box**	**Custom**
			Response	
2.9	Fallback	In the event of fallback, must the entire repository be restored to a frozen configuration or can selective fallback be done by backing out of changes to selected artifacts only?		
2.10	Custom Rules	What facilities exist for adding custom rules and/or behaviors to vendor-supplied artifacts and to user-supplied artifacts (e.g., naming standard enforcements and validation rules) to augment those that come "out of the box" as part of the software?		
2.11	Import/Export	Does your product have import and export capabilities in existing standards like XML or MY? Please describe which standard interchange formats you support.		
2.12	Deployed to Web	Explain how content is staged and deployed to the web. Is a separate deployment engine required? Can the product upload content from the staging area in bulk or piece by piece?		
2.13	Audit	Does the repository support change impact query/reporting of all artifacts?		
2.14	Access to Analytics	Do you support direct access to your repository from analytics tools? If so, which ones?		
2.15	Change Audit	Is it possible to generate, display and print version comparison reports detailing the changes made between two collections of artifacts (such as the changes reflected in all artifacts in a production version versus the previous version that had been in production)?		
2.16	Relational Inquiries	Is it possible for a user to stack paths of relational inquiries between repository artifacts and report them in a single report?		
2.17	Associated Configurations	Does your repository allow for artifacts and aggregates of artifacts to be associated with one or more configurations (e.g., Test Environment, Development Environment, Training Environment, Production Environment)?		
2.18	Business Rules	Does your product enable the creation of any business rule by business users without any product technical supervision?		
2.19	Graphic or Video	Can graphical and/or video images be used as part of the documentation of an artifact?		
2.20	Repository Generation	Please list all the things that the repository generates (e.g., DAB and Oracle database schemas, COBOL copybooks, transaction maps).		
3 Cost				
3.1	Initial Costs	Please provide a breakdown of costs associates with getting the solution up and running		
3.2	Ongoing Costs (Annual fees)	List annual fees such as licensing and maintenance costs		
3.3	Optional Components	Please provide additional list prices and volume discounts for any optional components (such as parsers, bridges and		

Placing a "Y" in the Out of the Box column indicates that the functions are contained in the solution proposed. Placing a "Y" in the Custom column indicates that a custom modification will be required. Please provide specific answers to questions in the response cells and if needed on a separate document. Reference the question number from the table below.				
1	**Feature**	**Description and/or Clarification**	**Out of the Box**	**Custom**
			Response	
		generators) and services that you offer beyond the basic software.		
3.4	Government Discount	What are the discount schedules available to governmental institutions?		
3.5	Cost Credits	Can costs associated with the initial implementation be accredited toward future upgrades to additional volume purchases or upgrades to site licenses?		
4 Services				
4.1	Support	Do you provide help-desk support 24 hours a day, seven days a week?		
4.2	Support Service Levels	Does your firm price support services based on your ability to meet user-defined service levels and speed (e.g., a different price for guaranteed responses within 24 hours)?		
4.3	Service Access Options	Are your support services available by phone, online, video conference and dispatched to the customer site?		
4.4	Client Environment Replication	Does your firm have a work center to replicate, in a managed environment, the potential problems that could occur in client accounts?		
5 Viability				
5.1	Growth	Have you experienced continued growth in new product sales and maintenance revenue over the past five years? Please provide details, if possible.		
5.2	Net Margins	Is your firm profitable? If yes, what are your net margins to the closest percent?		
5.3	Certification of third-party	Do you provide a certification process for third-party service providers? If so, please describe it.		
5.4	Sub-Contractors	Will you use sub-contractors for the solution proposed? If so, please list where they are located.		
6 Vision				
6.1	Investment Priority	Concerning your vision to improve these four areas, which one of the four do you plan to invest in most: (1) functionality; (2) cost; (3) service and support; and (4) ability to execute?		
6.2	Market Trends	What are three important emerging trends in your market and how do you envision incorporating these trends into your products?		
6.3	Future Enhancements	What major enhancements have you announced for delivery over the next 12 months?		
6.4	User Input	What vehicle is there for users to provide feedback on their product needs and impact the priorities assigned to product research development direction?		
6.5	User Groups	Do you have one or more user groups? If so, how many total member companies are there? Please list the available groups, where they are geographically located, and frequency of meeting.		

Placing a "Y" in the Out of the Box column indicates that the functions are contained in the solution proposed. Placing a "Y" in the Custom column indicates that a custom modification will be required. Please provide specific answers to questions in the response cells and if needed on a separate document. Reference the question number from the table below.				
1	**Feature**	**Description and/or Clarification**	**Out of the Box**	**Custom**
			Response	
6.6	New vs. Current Customer	Over the past three years, what percentage of your new product revenue comes from new customers versus older customers who are buying upgrades and are part of your installed base?		

Appendix 3 — Solution Requirements

Solution Name	Solution Needs to:
Deferred Comp	Current changes to deferrals have to be processed manually, too many carrier choices and date driven system makes changes difficult. E.g. start date always needs to be beginning of pay period, end date always needs to be at end of pay period. System sometimes does not stop calculations without the flags in the pay period to calculate. We would like the system to be able to handle changes and updates as they happen.
Minimal Technical Customizations	Provide 90% of requirement without additional customizations.
Updates for Regulatory Changes	Be able to adapt to frequent regulatory changes and apply Best Business practices as they are needed.
Manages and Updates Payrates	Be able to create pay scales without using secondary systems. For example, user should be able to select several (not all) paygrades and ask the system to automatically calculate a 1.5% increase for just the selected pay grades.
Talks to Other Systems	Be able integrate with secondary systems, and/or updates from secondary systems should easily transfer to the HRIS, so new employees don't have to be manually added to secondary systems and vice versa. For example, easier/automated adding of new employees and data transfer to other systems (e.g. Halogen).
Allows updating F/T and P/T pay	Be able to mass update pay rates in employee records, including part time employees.
Handles variances in process, policies, practices.	Be able to accommodate variances based on the County 's complex Union environment, i.e. pay practices, accruals, overtime calculations, shift and differential pay, pay rates, etc...
Date Adjustments Made Easier	Be able to recognize what dates needs to be adjusted based on the event we are entering. For example, when someone has an employment change in status, the system would automatically update all applicable fields with adjusted dates.
Creates a Positive Pay file for KeyBank	This is an important control that our current solution is currently unable to do out of the Payroll Module
More superuser flexibility, superuser needs to be able to make changes.	Be able to make changes or set parameters for functions without having to contact the vendor and waiting for vendor to update. E.g. Social Security Number changes, Provider changes, etc...
Support Multiple Union Environments	Be able customize employee's benefits, pay, and leave accrual based on their union designation.
Support Multiple Special Purpose Districts	Be able to have Special Purpose districts access the correct layer of information for themselves, without assistance from payroll staff
Run Multiple versions of Payroll	Be able to run multiple Payroll versions for county (bi-weekly) and special purpose districts (monthly)

Appendix 4 — Kitsap County Security Policy

Information Protection Policy

Description and Justification

Kitsap County's information is designated according to the Information Classification Policy, which confers restrictions on the systems that contain and the networks that transport that information. Each class of information requires certain protections during its use, storage, and transmission.

This Information Protection policy applies to all information stored or transported by County computing resources. Use of these resources is governed by the Kitsap County Information Technology Security Policy and Acceptable Use Agreement, regardless of the point of access.

General Protections

- The following controls are REQUIRED:
- Information must reside on appropriately accredited systems.
- Removable media must be labeled with County identification and classification.
    - If class 4 data must be stored on a removable device, that device must be encrypted and will be provided by CNS. This device must be returned to CNS when no longer needed.
- Information must be backed up when changed, or at most daily.
- Backup media must be secured in transport and storage.
    - Backup media is transported by authorized employees only
    - Backup media is transferred non-stop to and from storage facility
- Periodic backups must be kept at an approved storage facility.
    - Backup media is stored in an offsite secure County facility with controlled access.
    - Backup data is stored on tape locally and remotely at CENCOM and in the cloud

All required actions must be recorded in an audit log, including the authorized user, date, and time. Audit logs are classified as internal information.

Access is restricted to County employees and approved partners.

When media is no longer useful it will be destroyed. Media is never released for reuse by unauthorized users.

- Tape Destruction
    - Tapes are used until they are no longer able to retain data
    - At this point they are destroyed by a licensed media destruction vendor. The tape destruction is witnessed by authorized personnel.
- Desktop and laptop hard drives
    - By policy, data is not to be kept on the devices' hard drives
        - If it is necessary to store class 4 data on a laptop, that laptop must be encrypted
    - All data is to be kept on our network storage
    - When a device is removed from service its hard drive is removed and destroyed (by physically destroying the device)
- Copy machines with hard drives
    - All hard drives are removed from the devices before the copiers leave the County facility
    - When a device is removed from service its hard drive is removed and destroyed (by physically destroying the device). The hard drive destruction is witnessed by authorized personnel.

Protection policies for each information class

Protection	Description
Encryption	Use of county standard cryptography methods to obscure information from unauthorized users
Access Control	Restrict use of information to authorized people
Media	Data storage type or class

Policy	Description
Prohibited	Protection cannot be used
Allowed	Protection may be used, but is not required
Required	Protection must be used

Class 1 – Public Information

Protection	Policy
Encryption	
Storage	Allowed
Transport – internal	Allowed
Transport - external	Allowed
Backup	Allowed
Removable media	Allowed
Workstation	Allowed
Laptop	Allowed
PDA or phone	Allowed
Access control	
Read	Prohibited
Write	Required
Delete	Required
Media	
Removable	Allowed
Workstations and laptops	Allowed
PDA or phone	Allowed

Class 2 – Internal Information

Protection	Policy
Encryption	
Storage	Allowed
Transport – internal	Allowed
Transport – external	Required
Backup	Allowed
Removable media	Allowed
Workstation	Allowed
Laptop	Required
PDA or phone	Required
Access control	
Read	Allowed

Protection	Policy
Write	Required
Delete	Required
Media	
Removable	Allowed
Workstations and laptops	Allowed
PDA or phone	Allowed

Class 3 – Sensitive Information

Protection	Policy
Encryption	
Storage	Allowed
Transport – internal	Required
Transport – external	Required
Backup	Required
Removable media	Required
Workstation	Required
Laptop	Required
PDA or phone	Required
Access control	
Read	Required
Write	Required
Delete	Required
Media	
Removable	Allowed
Workstations and laptops	Allowed
PDA or phone	Allowed

Class 4 – Confidential Information

Protection	Policy
Encryption	
Storage	Allowed
Transport – internal	Required
Transport – external	Required
Backup	Required
Removable media	Required
Workstation	Required
Laptop	Required
PDA or phone	NA
Access control	
Read	Required
Write	Required
Delete	Required
Media	
Removable	Allowed if encrypted
Workstations and laptops	Allowed
PDA or phone	Prohibited

Secure Data Transfer Policy

Description and Justification

Secure Data Transfer Policy is required for all HIPAA, Criminal Justice Information System (CJIS), Personal Health Information (PHI) and Personal Identifying Information (PII).

This policy pertains to all Kitsap County employees, business associates, contractors and vendors.

General Protections:

The following controls are REQUIRED:

- Information must reside on appropriately accredited systems.
- Removable media must be labeled with County identification and classification
- Refer to Kitsap County Information Retention Policy for the backups and retention or destruction of confidential information.
    - Contract Language
        - Any external vendor/provider/agency that receives, handles, or stores County owned PHI or PII must have a signed contract with Kitsap County Risk Department
    - Backups
        - Refer to Kitsap County Information Retention Policy for the backups and retention or destruction of confidential information.
        - Backups stored in a secure location
        - Transport between source and storage location must be non-stop
    - Electronically transmitted data must be encrypted during transport and at rest
- Secure Transport
    - Valid methods of secure transfer or transmission includes but is not limited to: SFTP, VPN, HTTPS, etc.
    - Invalid methods of transfer or transmission includes modes where data is sent in “clear Text” (including but not limited to: FTP, TELNET, HTTP, etc.)
    - Email
        - All email containing PHI or PII must be sent encrypted
            - All email between County employees within our County email system is encrypted
            - All email sent outside our County email system must be sent encrypted via Barracuda or other approved encrypted delivery service
            - All email sent outside our County email system must include a confidentiality notice
        - If you receive an unencrypted email that contains secure data. Only reply to the email with an encrypted email. Let the sender know that the information contains secure data and it was received in an unsecure manner. (We cannot control how someone sends inbound email, but we cannot continue the communication with an unsecure transport.)

HIPAA Specific

- All vendors/providers/agencies receiving, handling or storing Kitsap County PHI or PII must have a signed Business Associate Agreement on file.

CJIS Specific

- We do not store CJIS data on our servers or personal devices. Therefore, it is (against Secure Data Transfer Policy and) not possible to send it in any form.

Event Logging Policy

Description and Justification

Kitsap County servers and network devices store and transport public, internal, sensitive, and confidential information. To ensure the integrity of these systems, it is necessary to monitor and record administrator activities.

The purpose of the Event Logging Policy is to describe the requirements for recording administrative activities that may impact the integrity of systems. While the primary use of logs is forensic investigation or validation, logs may be use for problem detection.

This policy applies to all servers and network devices that store, process, or transmit Internal, Sensitive, or Confidential information.

Required Safeguards

Responsible event logging REQUIRES:

- Servers and devices to keep a log of all administrator actions, including:
    - Configuration changes
    - Permission changes
    - Administrator account changes
    - Successful and unsuccessful administrator log on attempts
- Administrators each use unique accounts whenever practicable.
- Accounts used for server and device administration are not used for non- administrative activities.
- Servers or devices to keep a log of suspicious user activities, including:
    - Excessive failed log on attempts
    - Permission change attempts
    - Attempts to access known inappropriate content
    - Other events deemed suspicious by IT staff
- Servers and devices maintain synchronized time.
- Log entries include:
    - Date and time
    - System name and address
    - User id, when applicable
    - Event id
    - Event description
- Complete log data will be kept for 1 year.
- Log data will be reviewed at least weekly by qualified IT staff. IT staff may use appropriate log analysis automation tools. IT staff will investigate findings as appropriate.
- Reports will be made available to IT management at least monthly, or on request.
- Reports will include:
    - Total events
    - Summary of servers and devices
    - Summary of administrator events
    - Summary of suspicious user activities
    - List of follow-up actions completed and planned

Network Security Policy

Description and Justification

Kitsap provides access to many of its critical computing resources from the Internet, the Intergovernmental Network (IGN), networks of affiliated governments and agencies in order to facilitate convenient access to information and communications for citizens, and staff of the County and partner agencies. This includes access to sensitive and private information. All users must recognize their responsibilities in protecting information that is accessible via the Internet and other networks.

This policy applies to all access from the Internet, IGN, or other non-County networks to County computing resources. Use of these resources is governed by the Kitsap County Information Technology Security Policy and Acceptable Use Agreement, regardless of the point of access.

Prohibited Activities

The following actions relating to Internet security are PROHIBITED:

- Any attempt to access information, or to modify or destroy data or passwords belonging to other users, even if that information is not properly protected by its owner.
- Providing network access to computers or software not explicitly approved by the DIS Director. This includes using remote access software (e.g., PC Anywhere, GoToMyPC.com, etc.).
- Using public computers to access protected information. This includes computers provided publicly at libraries or Internet cafes.
- Forwarding, copying, or local storage of sensitive information.

Required Safeguards

Responsible use of access to County resources from the non-County networks REQUIRES:

- That all network-accessible systems comply with the Server Accreditation Policy. This includes secure authentication, appropriate access controls, data encryption, and secure system configuration and maintenance.
- DIS to provide technical safeguards that prohibit all access from the non-County networks, except for explicitly approved servers and applications.
- That web pages and other documents that contain private or sensitive information be appropriately labeled.
- Users to take exceptional care not to disclose passwords or other credentials used to access County resources and to comply with the Password Policy.
- That users report observed misuse of County systems, as well as information or situations that may lead to misuse.

Physical Security Policy

Description and Justification

Kitsap County computers and networks provide services critical to operations. Protecting equipment that contains or transports County information from loss, damage, or tampering is a fundamental information protection.

This policy refers to the protection of building sites and equipment (and all other information and software contained therein) from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage (e.g., from electrical surges, extreme temperatures, and spilled coffee).

Facility Classifications

Class	Name	Description
1	Public	Areas or buildings without access controls
2	Office	Employee work areas. Access is restricted to employees and escorted guests.
3	Communications Room	Rooms that contain network and telecommunication equipment to support local network connectivity. Devices do not contain any general purpose storage. May be shared with other facilities infrastructure, such as fire alarms.
4	Datacenter	Rooms that contain servers and network core devices.

Class 1 – Public

The following actions relating to public facilities are PROHIBITED:

- Provision of network connections (wired or wireless) that provide unencrypted access to internal networks.
- Persistent storage of any Internal, Sensitive, or Confidential information.

The safeguarding equipment in public facilities REQUIRES:

- Workstations designed for secure public access:
  - Physically protected from theft or vandalism.
  - No active input/output ports available, including wireless access, like Bluetooth.
  - Software that deletes user information between sessions.
  - Labeled as property of the County.
  - Posted with notice of acceptable use.
  - Annual inventory verification.
- Non-portable employee workstations used in public areas require:
  - Physically protected from theft or vandalism.
  - No active input/output ports available, including wireless access, like Bluetooth.
  - Access control that permits use only by employees.
  - Encrypted data storage.
  - Encrypted network access.
  - Control of displays, including positioning, partitions, or viewing angle filters, to inhibit view of sensitive data by non-employees.
  - Labeled as property of the County.
  - Posted with notice of acceptable use.
  - Annual security awareness review by employees using public area workstations.
  - Annual inventory verification.
- Portable employee workstations using in public areas require:
  - Accreditation.
  - Access control that permits use only by employees.
  - Encrypted data storage.
  - Encrypted network access.
  - Annual security awareness review by employees using public area workstations.
  - Annual inventory verification.

Class 2 – Office areas

The following actions relating to office facilities are PROHIBITED:

- Persistent storage of any Sensitive or Confidential information.
- Location of any servers, network devices, or communication service demarcation.

The safeguarding equipment in office facilities REQUIRES:

- Access controlled by physical controls (locks) or human monitoring.
- Employee workstations for office areas require:
    - Accreditation.
    - Access control that permits use only by employees.
    - Labeled as property of the County.
    - Annual security awareness review by employees.
    - Annual inventory verification.

Class 3 – Communication Rooms

The following actions relating to communication rooms are PROHIBITED:

- Location of any servers.
- Storage of unused equipment or other material.

The safeguarding equipment in communication rooms REQUIRES:

- Physical access controls.
- Maintaining an access log.
- Equipment must be secured to the building structure.
- If the room is shared, equipment must be in locked cabinets.
- Fire controls.
- Posting of authorized access-only notices.
- Posting of emergency contact information.

Class 4 – Datacenters

The following actions relating to datacenters are PROHIBITED:

- Storage of unused equipment or other material.
- Bringing in food, beverages, or other liquids.

The safeguarding equipment in communication rooms REQUIRES:

- Physical access controls.
- Maintaining an access log.
- Equipment must be secured to the building structure.
- Non-water fire controls.
- Control for water damage from fire sprinklers or plumbing.
- Power conditioning and monitoring.
- Air filtration and dust control.
- Backup power for 24 hours for systems and environmental controls.
- Temperature and humidity control and monitoring.
- Posting of authorized access-only notices.
- Posting of emergency contact information.

Remote Access Policy

Description and Justification

Access to County computing resources from the Internet has inherent risks. Users permitted remote access are responsible for specific measures to maintain the confidentiality of sensitive information while using remote access.

This policy governs all access to County computer resources from the Internet or other non- county networks. Remote access for telecommuting is also governed by the Kitsap County Telecommuting Policy Guide, Resolution 075-1998.

Prohibited Activities

The following uses of County remote access are PROHIBITED:

- Circumventing remote access control, authentication, or encryption software.
- Storing County information on non-county computers.
- Installation of software licensed to the County on non-County computers.

Required Safeguards

Responsible use of County remote access REQUIRES:

- Use of County computers or non-county computers with properly installed and configured, authorized anti-virus and firewall software.
- Due care in protecting passwords and credentials for remote access. Readable usernames or passwords cannot be kept with computers used for remote access.
- Users be aware that by using their personal equipment for remote access to County systems, they are consenting to search of that equipment, if required to satisfy public disclosure.

Security Incident Response Policy

Description and Justification

Kitsap County's information is critical to its mission. Disclosure, corruption, or loss of information will negatively impact the County and the safety of citizens and staff.

A security incident is defined as:

- Any potential violation of federal, state, or county law, or Kitsap County policy involving a County information asset.
- A breach, attempted breach or other Unauthorized Access of a County information asset. The incident may originate from the County network or an outside entity.
- Any Internet worms or viruses.
- Any conduct using in whole or in part a County information asset which could be construed as harassing, or in violation of County policies.

This Security Incident Response policy applies to all information stored or transported by County computing resources. Use of these resources is governed by the Kitsap County Information Technology Security Policy and Acceptable Use Agreement, regardless of the point of access.

Required Safeguards

Security Incident Response Requires:

- Establishing and maintaining a plan for effectively managing DIS resources during a security incident, including:

        - Roles and responsibilities
        - Priorities for preserving evidence versus service recovery
        - Damage assessment procedures
        - Communication procedures with staff, management, users, partners, and the public
        - Plan maintenance procedures
    - Train DIS staff for security incident response roles.
    - Conduct security incident exercises at least annually.
    - Obtain a third party audit of the plan at least every 3 years.

Vendor Access Policy (including VPN Access)

Description and Justification

Vendors play an important role in the support of hardware and software management, and operations for customers. Vendors can remotely view, copy and modify data and audit logs, they correct software and operating systems problems, they can monitor and fine tune system performance, they can monitor hardware performance and errors, they can modify environmental systems, and reset alarm thresholds.

Setting limits and controls on what can be seen, copied, modified, and controlled by vendors will eliminate or reduce the risk of loss of revenue, liability, loss of trust, and

embarrassment to Kitsap County.

This policy applies to all servers and network devices that permit direct access by Vendors for maintenance and operations.

Prohibited Activities

The following actions relating to vendors are PROHIBITED:

- Access of systems or information that are not specified within the scope of the vendor agreement.

Required Safeguards

Responsible vendor access REQUIRES:

- Vendors must comply with all applicable County policies, practice standards and agreements, including, but not limited to:
    - Safety Policies
    - Information Protection Policy
    - Network Security Policy
    - Auditing Policies
    - Software Licensing Policies
    - Acceptable Use Policy
    - Vendor agreements and contracts must specify:
        - The County information the vendor should have access to
        - How County information is to be protected by the vendor
        - Acceptable methods for the return, destruction or disposal of County information in the vendor's possession at the end of the contract
        - The Vendor must only use County information and resources for the purpose of the business agreement
        - Any other County information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or divulged to others
    - County will provide a DIS point of contact for the Vendor. The point of contact will work with the Vendor to make certain the Vendor is in compliance with these policies.

- Each vendor must provide County with a list of all employees working on the contract.

The list must be updated and provided to County within 24 hours of staff changes.

- Vendor personnel must report all security incidents directly to the appropriate County personnel.
- If vendor management is involved in County security incident management, the responsibilities and details must be specified in the contract.
- Vendor must follow all applicable County change control processes and procedures.
- Regular work hours and duties will be defined in the contract. Work outside of defined parameters must be approved in writing by appropriate County management.
- VPN access for vendors is disabled by default.
- Vendor must inform DIS when access is required.
- County sponsor must sign off before vendor access is granted

User Account Password and Credential Policy

Description and Justification

Passwords are the primary method for authenticating users to County computer resources. Anyone who possesses another person's password may view, modify, or destroy any information to which the owner is permitted to view, modify, or destroy. Because computer systems have no other way of recognizing a user, disclosure of a password may be more harmful than unauthorized access to building keys, private documents, or other County resources.

Protecting passwords is one of the most important responsibilities for each user. Passwords can be illegitimately disclosed by sharing, copying, or guessing. Each user accepts responsibility for taking reasonable precautions to safeguard his or her passwords.

Prohibited Activities

The following actions relating to passwords are PROHIBITED:

- Sharing a password. All users are permitted access to the computer resources that they legitimately need with their own account and password. Information Services staff should NEVER ask for a user's password, but if the password is revealed it must be changed on the next login.
- Sending passwords through email.
- Any attempt to guess, copy, or otherwise obtain passwords belonging to other users.
- Use of another user's password, even if shared or left unprotected.
- Storing a password in a public location. This includes desktops, unlocked drawers or cabinets, and unprotected electronic documents.

Required Safeguards

Responsible use of passwords REQUIRES:

- Passwords MUST be changed regularly, in accordance with the following parameters:

Class	Password Holder	Frequency
1	General users, Employees, managers, elected officials, vendor users, Department Heads, managers, and Information Services staff	Every 90 days
2	System administrator accounts	Every 4 months
3	Service accounts	Never

- Passwords MUST be changed when requested by Information Services staff.
- Passwords MUST be changed, and supervisor notified, if unauthorized disclosure is suspected.
- Notification of supervisor when aware of possible password misuse.
- Passwords MUST be sufficiently obscure, in accordance with the following parameters:

Active Directory	
Minimum length (characters)	8
Character set	A-Z a-z 0-9 ~!@#$%^&*_+-=
Character combinations	Not similar to username Not an English word Not in common password dictionary Cannot match any of the previous 10 passwords
Storage	MAY be written and stored in secure physical location

IBM iSeries (Financial Management System)	
Length (characters)	6 -10
Character sets	A-Z a-z 0-9 $@#_
Character combinations	Not similar to username Not an English word Not in common password dictionary Cannot match any of the previous 32 passwords
Storage	MAY be written and stored in secure physical location

- The Department of Information Services MUST:
    - Classify password databases at the same or higher risk level as the information such databases protect and take appropriate safeguards.
    - Whenever possible ensure that applications use Active Directory account authentication.
    - Ensure that Non-Active Directory applications are periodically reviewed for compliance by the application's administrator.
    - Configure systems and applications to conform to user password policies.
    - Configure systems and applications to permit no more than five (10) unsuccessful login attempts before locking out the user/account for at least one (1) hour.
    - Provide convenient password change mechanisms, including timely password reset in the event of a forgotten password.
    - Periodically audit the password policy for compliance.
    - Provide secure electronic password storage for staff.

Information Retention Policy

Description and Justification

Kitsap County complies with the Washington State CORE standards.

Prohibited Activities

Data is not allowed to be deleted outside its retention date as described in the CORE.

Virus Protection Policy

Purpose

Kitsap County shall promote a secure computing environment for all users of the County network. Computing platforms (including but not limited to: desktop workstations, laptops, hand-held, personal digital assistants, servers and network devices) are integral elements in the operations of the County and as such are vital to the County's mission. This policy

will help ensure that all vulnerable computing platforms are guarded against vulnerabilities and protected by antivirus software at all times.

Scope

This document describes the measures taken by the County to counter computer viruses and identifies the responsibilities of individuals, departments and The Information Service's Computer & Network Services Division (CNS) in protecting the County against viruses and other vulnerabilities.

Objectives

The principal concern of this computer virus protection policy is effective and efficient prevention of all network virus outbreaks and network security attacks involving all computers associated with Kitsap County. The primary focus is to ensure that Kitsap County employees and partnering agencies are aware of and take responsibility for the proper use of the County-provided and CNS-supported virus protection software. This policy is intended to ensure:

- The integrity, reliability, and good performance of County computing resources;
- That the user operates according to a minimum of safe computing practices;
- That the County licensed virus software is used for its intended purposes; and
- That appropriate measures are in place to reasonably assure that this policy is honored.

Policy Statement

Any computer, server or network devices connected to the Kitsap County network shall be protected by antivirus software from malicious electronic intrusion. This policy applies to all devices connected, by any means, to the Kitsap County network including those owned by the County, employees, partnering agencies, and third-party vendors.

All computers or networked devices shall have applicable operating system and application security patches and updates installed prior to initial connection to the network.

Additionally, those personal use systems for which antivirus software is available shall have it installed and configured for effective operation prior to their connection to the County network.

CNS is solely responsible for the purchase of antivirus software for all Kitsap County computers, servers, or any network device connected to the Kitsap County network.

How viruses can infect Kitsap County's network

There are three types of computer viruses: true viruses, Trojan horses, and worms. True viruses actually hide themselves, often as macros, within other files, such as spreadsheets or Word documents. When an infected file is opened from a computer connected to Kitsap County's network, the virus can spread throughout the network and may do damage. A Trojan horse is a program file that, once executed, doesn't spread but can damage the computer on which the file was run. A worm is also a program file that, when executed, can both spread throughout a network and do damage to the computer from which it was run.

Viruses can enter Kitsap County's network in a variety of ways:

- E-mail — Web links in emails are a popular way of infecting PCs and networks. Never click on a link in an email you did not request or was not expecting. If you receive an email unexpectedly and are requested to click on a link or visit a web site, contact the sender to ensure it is a legitimate email. Also, never open an attachment in a suspicious email. These attachments could be working documents or spreadsheets, or they could be merely viruses disguised as pictures, jokes, etc. These attachments may have been knowingly sent by someone wanting to infect Kitsap County's network or by someone who does not know the attachment contains a virus. However, once some viruses are opened, they automatically e-mail themselves, and the sender may not know his or her computer has been infected.
- Disk, CD, Zip disk, or other media — Viruses can also spread via various types of storage media. As with e-mail attachments, the virus could hide within a legitimate document or spreadsheet or simply be disguised as another type of file.
- Visiting an infected web site — Cyber Security firms attest: most web sites are infected. Kitsap County users should assume that most web sites are infected and should only visit web sites directly related to County business.
- Software downloaded from the Internet — Downloading software via the Internet can also be a source of infection. As with other types of transmissions, the virus could hide within a legitimate document, spreadsheet, or other type of file. Downloading software from the Internet is prohibited (Electronic Use Policy). If you need software installed on your PC contact the Help Desk.

Computer & Network Service's Responsibilities

Obligation and Usage

- CNS purchases antivirus software and licenses for all Kitsap County computer systems.
- Installation of the antivirus software is required on ALL County owned machines. This product is provided to all County computers, servers, and network devices. Product
- is configured to automatically receive virus definition updates from a centralized- managed server.
- Deployment of anti-virus software.
- CNS staff installs the antivirus software on the images used for all computers. The software is available for all computers running on the network.
- CNS will keep the anti-virus products it provides up to date. We utilize the antivirus software with centralized policy management. This allows us to automatically deploy new virus definitions to workstations connected to the domain.
- Centrally-managed virus protection software provided by CNS will run on all Kitsap County computers, servers, or any appropriate network device connected to the Kitsap County network.

Containment of Virus incidents

- CNS staff will take appropriate action to contain virus infections and assist in their removal. In order to prevent the spread of a virus, or to contain damage being caused by a virus, CNS may remove a suspect computer from the network or disconnect a segment of the network.
- CNS will provide advice to individuals on the function and installation of the anti- virus products and on virus protection. This includes advice on virus hoaxes, including occasional emails on specific hoaxes.
- CNS is responsible to recover from viruses. This includes containment, removing viruses, restoring device to proper working condition. Unfortunately, the process of restoring the device will result in the disk drive being rebuilt. This means anything on the hard drive will be lost including desktop icons and favorites.

Server Accreditation Policy

Description and Justification

Kitsap County servers store public, internal, sensitive, and confidential information, as described in the Information Classification Policy. Servers are depended upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability are maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service.

The purpose of the Server Accreditation Policy is to describe the requirements for installing a new server in a secure fashion and maintaining the security integrity of the server and application software.

This policy applies to all access servers that store, process, or transmit County information.

Prohibited Activities

The following actions relating to servers are PROHIBITED:

- Attaching non-accredited servers to the network
- Storing information on servers that are not accredited for the appropriate information classification.

Required Safeguards

Responsible management of servers REQUIRES:

- Servers be accredited:
    - When originally deployed
    - Annually
    - Immediately if principal applications or operating system software is added or upgraded a major version
    - Immediately if server function, user roles, or access scope changes.
- Information stored, processed, or transmitted by a server must the described in detail and classified according to the Information Classification Policy. Any change in the type of information stored, processed or transmitted by a server requires that the server be re-accredited.
- User and administrator roles for the server be described in detail. Policies concerning role permissions and responsibilities must be established.
- Each server to have a specified data custodian, responsible for information accuracy, access controls, and timeliness.

- Each server must be configured according to County DIS procedures according to classification. Procedures address:
    - Installation of operating systems from an approved source.
    - Application of operating system vendor security patches.
    - Application of other DIS approved or required vendor patches.
    - Removal of unnecessary software, system services, and device drivers.
    - Configuration of system security parameters, auditing, firewall settings, and file permissions.
    - Removal of unnecessary local accounts and reset passwords on built-in and service accounts in accordance with County Password Policy.
    - Configuration user authentication and authorization methods.
- Each server must have written maintenance procedures and be maintained according to those procedures, including:
    - Access approval, initiation, modification, and termination for user and administrator roles.
    - Change control procedures, including testing, incident response, troubleshooting, and production change.
    - Disaster recovery procedures, including back-up and restore, business impact analysis, and full system recovery.
    - Timely application of IT-required vendor patches.

Servers must be located in IT-specified physically secure locations

PC, Laptop, and Server Build Policy

Description

PCs, laptops, and servers are received new from the vendor by the CNS department only. If these devices are to be reused, they must be processed by the CNS department before repurposed. If any of these devises are to be decommissioned, the CNS department must process them before they leave the County's possession.

General Protections

PCs and Laptops

- New
    - New PCs and Laptops are ordered through our Purchasing department with CNS' approval.
    - The devices are shipped directly to the CNS department and built according to the policies described in this document.
    - All laptops are built with encrypted hard drives.
- Repurposed
    - When a PC or laptop is to be reused by a different user it must be sent to CNS for rebuilding.
    - The device is totally wiped for security purposes.
    - Even though there is not supposed to be data on the device's hard drive, it must be wiped to ensure no data is accidently left on the device.
    - The device is built as if it were a new device.
- Retired
    - When a device is decommissioned the hard drive is removed from the device and physically destroyed by CNS staff.
    - The device is destroyed, not given away or donated.

Physical Servers

- New
    - Servers are ordered through our Purchasing department with CNS' approval.
    - The devices are shipped directly to the CNS department and built according to the policies described in this document.
    - These servers are placed in service in a designated server room.
- Repurposed
- When a server is to be repurposed the O/S must be reloaded.
    - If the server has internal disk drives they must be totally wiped for security purposes after they are backed up for retention purposes (if necessary).
    - The device is built as if it were a new device.
- Retired
    - When a server is decommissioned the hard drives must be removed from the device and physically destroyed. Any deviation from this policy must have management approval.
    - The device or its components may be kept in inventory if it is of any value.
    - If the device is to be decommissioned its disk drives must be removed and physically destroyed by CNS staff.
    - The device is destroyed, not given away or donated.

Appendix 5 — Kitsap County Security Questionnaire

DATA

1. Where is the data stored?
2. Who owns the data?
3. What is the capability of exporting the data when contract is complete/over?
4. Export mechanism for getting data base to the county?
5. How far back to recover a record?
6. Storage cost? What comes with package and what is the growth cost?
7. Discovery/disclosure requests? – How long is data kept?
8. Procedure for Discovery disclosure to the vendor?

Data Security

1. Backup/restore plan?
2. D/R plan?
3. SLA for ISP?
4. Data encrypted in transit?
5. Data encrypted at rest?
6. Authentication to S/W
7. ADFS integrated? Single sign on?
8. Is not ADFS would the end users be capable of managing their own users?
9. Logging, do you maintain access logs, data time log out, etc.
10. Confidential information not to be made public?
11. Security roles? Who manages new users, is it role based? P/M, user, administrator, etc.

Application Needs

1. Bandwidth needed?
2. What is your app. support experience? Handle all calls from all users or one point of contact in **Kitsap County to call you?**
3. Does this app work with mobile devices?
4. Is it an app or an installed client?
5. Do you provide APIs or web services data integration or extracting data?
6. Do you provide a developer's tool kit?
7. Is there anything you would be exposing to the public from our data set?
8. Legal venue? Washington
9. Renewal and termination (notice duration for renewals)?
10. Do you employ any sub-contractors – like outsource support?

11. Is there any customization needed to bring us on board?

12. What reporting tools do you use? Management reports, P/M reports, ad hoc reports (can we create them or do you have to)? Add on cost to add more reports later?

13. Project Status alerts? Work with our O365 Exchange email system?

14. Do you provide work flow diagrams of the work processes?

This document is designed to be an interactive communication tool. The purpose of these questions is to enable deeper discussion based on these answers. It is not a document a vendor can fill out and return expecting it to be complete.