

CITY OF BELLEVUE



REQUEST FOR PROPOSAL RFP # 12289

IP Camera and NVR Solution

Issue Date: December 5, 2012
Due Date and Time: December 19, 2012 no later than 4:00 p.m. PST

REQUEST FOR PROPOSAL

Notice is hereby given that proposals will be received by the City of Bellevue, Washington for:

RFP # 12289

IP Camera and NVR Solution

by filing with the Contracting Services office of the Finance Department, 450 110th Avenue NE, Bellevue, Washington, 98004 until:

Date: **December 19, 2012**

Time: **4:00 p.m. PST**

Proposals submitted after the due date and time may not be considered. Vendors accept all risks of late delivery of mailed proposals regardless of fault.

Detailed Request for Proposal (RFP) information including general information, general terms and conditions, requested services, proposal requirements and evaluation process is available from the Contracting Services office located at the above address or by calling (425) 452-7876. The RFP is also available on the City's website at www.cityofbellevue.org, under "Doing Business" and "Bid Information."

The City of Bellevue reserves the right to reject any and all submittals and to waive irregularities and informalities in the submittal and evaluation process. This RFP does not obligate the City to pay any costs incurred by respondents in the preparation and submission of a proposal. Furthermore, the RFP does not obligate the City to accept or contract for any expressed or implied services.

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

Dated this 5th day of December, 2012

Jamie Robinson
Procurement Services Supervisor

Published: Seattle Daily Journal of Commerce: December 5th and 12th, 2012
Seattle Times: December 5th and 12th, 2012

TABLE OF CONTENTS

Page

REQUEST FOR PROPOSAL	2
SECTION 1. GENERAL INFORMATION.....	5
1.01 INTRODUCTION.....	5
1.02 PURPOSE OF RFP	5
1.03 DEFINITIONS	5
1.04 RFP COORDINATOR/COMMUNICATIONS.....	5
1.05 PRELIMINARY SCHEDULE	6
1.06 RESPONSE FORMAT	6
1.07 COMPLETENESS OF PROPOSAL	6
1.08 PROPOSAL RESPONSE DATE AND LOCATION.....	7
1.09 REQUIRED NUMBER OF PROPOSALS	7
1.10 VENDOR'S COST TO DEVELOP PROPOSALS.....	7
SECTION 2. TERMS AND CONDITIONS.....	8
2.01 QUESTIONS REGARDING THE RFP	8
2.02 RFP CLARIFICATIONS & ADDENDUMS	8
2.03 WITHDRAWAL OF PROPOSAL	8
2.04 REJECTION OF PROPOSALS	8
2.05 CODE OF CONDUCT FOR SOLICITATIONS.....	8
2.06 PROPOSAL MODIFICATION AND CLARIFICATIONS	9
2.07 PROPOSAL VALIDITY PERIOD	9
2.08 PROPOSAL SIGNATURES	9
2.09 PUBLIC RECORDS.....	9
2.10 BUSINESS REGISTRATION AND TAXATION	9
2.11 NON-ENDORSEMENT	10
2.12 NON-COLLUSION CERTIFICATE	10
2.13 INSURANCE REQUIREMENTS	10
2.14 EQUAL OPPORTUNITY & TITLE VI REQUIREMENTS	10
2.15 NON-DISCLOSURE AGREEMENT	10
2.16 TECHNOLOGY RESOURCE USAGE POLICY.....	10
2.17 INFORMATION SECURITY REQUIREMENTS.....	10
2.18 OTHER COMPLIANCE REQUIREMENTS.....	10
2.19 OWNERSHIPS OF DOCUMENTS.....	11
2.20 COOPERATIVE PURCHASING	11
2.21 CONFIDENTIALITY OF INFORMATION.....	11
SECTION 3. REQUESTED SERVICES.....	12
3.01 DURATION OF SERVICES	12
3.02 VENDOR INFORMATION.....	12
3.03 PERFORMANCE EXPECTATIONS.....	12
3.04 SCALABILITY	12
3.05 COST REQUIREMENTS.....	13
SECTION 4. TECHNICAL ARCHITECTURE REQUIREMENTS	14
4.01 NETWORK.....	14
4.02 SERVERS AND OPERATING SYSTEM	14
4.03 CLIENT WORKSTATIONS.....	15
4.04 SYSTEM OPERATION AND MAINTENANCE	16
4.04.01 Application Security.....	16
4.04.02 Web Application Security.....	16
4.04.03 System Maintenance	16
4.04.04 Support.....	16
4.04.05 Support Staff Resources.....	17

4.04.06	<i>Licensing</i>	17
4.04.07	<i>System Interfaces and Connectivity</i>	17
4.04.08	<i>Upgrades</i>	17
4.04.09	<i>Data Storage</i>	17
4.05	SYSTEM IMPLEMENTATION	17
4.05.01	<i>Project Implementation and Training Plan</i>	17
4.06	CITY OF BELLEVUE DEPARTMENT EXISTING SETUP.....	18
SECTION 5. SCOPE OF SERVICES.....		19
SECTION 6. PROPOSAL EVALUATION AND VENDOR SELECTION.....		24
6.01	EVALUATION PROCEDURES.....	24
6.02	SCORING AND EVALUATION FACTORS	24
6.03	SELECTION PROCESS.....	24
6.04	CONTRACT AWARD AND EXECUTION	25
FORM #1 PROPOSAL FORM		26
FORM #2 VENDOR INFORMATION REQUIREMENTS.....		28
FORM #3 CLIENT REFERENCES		31
ATTACHMENT “A”		32
NON-COLLUSION CERTIFICATE		32
ATTACHMENT “B”		33
INSURANCE REQUIREMENTS.....		33
ATTACHMENT “C”		34
EQUAL OPPORTUNITY & TITLE VI REQUIREMENTS		34
AFFIDAVIT OF EQUAL OPPORTUNITY & TITLE VI COMPLIANCE		37
ATTACHMENT “D”		38
CITY OF BELLEVUE NON-DISCLOSURE AGREEMENT		38
ATTACHMENT “E”		42
PRICING		42
ATTACHMENT “F”		43
TECHNOLOGY RESOURCE USAGE POLICY.....		43
ATTACHMENT “G”		50
INFORMATION SECURITY REQUIREMENTS		50

Section 1. General Information

1.01 Introduction

The City of Bellevue is located three miles east of Seattle, between Lake Washington and Lake Sammamish, and about ten miles west of the foothills of the Cascade Mountain. The City's resident population of ~117,000 and daily workforce of ~121,000 make it Washington's fifth-largest city. Bellevue is a prosperous, increasingly diverse city that has evolved from a "bedroom community" into the economic and cultural hub of the Seattle area's Eastside. The City has developed its downtown core into a major business and retail center while maintaining the safe, comfortable family neighborhoods for which it has long been popular.

1.02 Purpose of RFP

The objective of this Request For Proposal (RFP) is to solicit proposals to provide the City of Bellevue (the City) with an implementation of the Avigilon Control Center Enterprise edition system solution for its IP Camera and NVR solution. All interested vendors, whether previously contacted or not, are required to submit proposals in accordance with the conditions and dates outlined in this Request for Proposal (RFP).

The City of Bellevue is planning to consolidate multiple software, DVR and camera systems into a standardized solution. This will include simplifying video retention policies and storage practices, providing growth capacity, and allowing increased video coverage of remote sites.

We are migrating from Analog to IP cameras, with a goal in reduced licensing fees, maintenance and other Vendor associated costs.

The City expects to develop a long-term, collaborative relationship with the selected Vendor for this solution.

1.03 Definitions

City	The City of Bellevue, Washington, and its departments.
Vendor	The person or firm submitting the proposal and/or the person or firm awarded the contract.
Contract	The agreement to be entered into for services between the City and the Vendor who submits the proposal accepted by the City.
RFP	This Request for Proposal, including any amendments or other addenda hereto.
Selection Committee	The RFP Selection Committee is comprised of the RFP Coordinator (defined in Section 1.04) and other City staff.
Short List	Vendors selected to proceed for further evaluation.

1.04 RFP Coordinator/Communications

Upon release of this RFP, all vendor communications concerning this information request should be directed in writing to the RFP Coordinator listed below. Unauthorized contact regarding this RFP with

other City employees may result in disqualification. Any oral communications will be considered unofficial and non-binding on the City.

RFP Coordinator for this RFP will be:

Name: Jeff Werdal
Address: City of Bellevue
Street - 450 110th Avenue NE
Mailing - P.O. Box 90012, Bellevue, WA 98009-9012
Telephone:.....425-452-6996
Fax:..... 425-452-7882
E-mail:..... jwerdal@bellevuewa.gov

1.05 Preliminary Schedule

These dates are estimates and are subject to change by the City.

Event	Time & Date
Release RFP to Vendors	12/5/12
Vendor RFP Questions (if any) Due	12/11/12 by 5:00 PM PST
Answers to Vendor RFP Questions Released	12/13/12
Proposal Responses Due	12/19/12 by 4:00 PM PST
Proposal Evaluation Complete	12/21/12
Vendor Reference Checks Complete	1/9/13
Vendor Finalists Announced	1/16/13
Announce Apparently Successful Vendor	1/18/13
Contract Negotiations complete	January 2013
Signed Contract Delivered To Vendor	January 2013
Installation Begins	February 2013

1.06 Response Format

Proposals should be prepared simply, providing a straightforward, concise delineation of the approach and capabilities necessary to satisfy the requirements of the RFP. Technical literature and elaborate promotional materials, if any, must be submitted separately. Emphasis in the proposals should be on completeness, clarity of content and adherence to the presentation structure required by this RFP.

Vendor proposals must be submitted in the format specified in Form #1 Proposal Form. Please provide responses in the format provided. **Vendors that deviate from this format may be deemed non-responsive.**

1.07 Completeness of Proposal

The vendor must attach the **Form #1 Proposal Form** signed by a vendor representative authorized to bind the proposing firm contractually. This statement must identify any exceptions that the Vendor takes to the City's RFP, or declare that there are no exceptions taken to the RFP. **Vendors that fail to complete this step may be deemed unresponsive.**

1.08 Proposal Response Date and Location

Proposals must be submitted to the City of Bellevue's Service First Desk no later than **December 19th, 2012 at 4:00 pm PST**. The Official Clock for submissions is located at the Service First Desk (address listed below). All proposals and accompanying documentation will become the property of the City and will not be returned. Faxed proposals will not be accepted. Vendors accept all risks of late delivery of mailed proposal regardless of fault.

The Service First Desk may be contacted at:

Office Location

Bellevue City Hall
450 110th Avenue NE
Bellevue, WA 98004
Ph: (425) 452-7876

Mailing Address

City of Bellevue
Service First Desk
P0 Box 90012
Bellevue, WA 98009-9012

1.09 Required Number of Proposals

A total of **one original, 5 copies and an electronic copy** of the vendor's proposal, in its entirety, must be received as specified in Section 1.08. The City, at its discretion, may make additional copies of the proposal for the purpose of evaluation only. The original proposal will include original signatures, in ink, by authorized personnel, on all documents that require an authorized signature.

1.10 Vendor's Cost to Develop Proposals

Costs for developing proposals in response to the RFP are entirely the obligation of the vendor and shall not be chargeable in any manner to the City.

Section 2. Terms and Conditions

2.01 Questions Regarding the RFP

Oral interpretations of the RFP specification are not binding on the City. Request for interpretation or clarification of the RFP specifications must be made in writing and submitted to the RFP Coordinator indicated in Section 1.04.

2.02 RFP Clarifications & Addendums

The City reserves the right to clarify or change the RFP or issue addendums to the RFP at any time. The City also reserves the right to cancel or reissue the RFP. All such addenda will become part of the RFP.

In the event that it becomes necessary to revise any part of this RFP, the City will issue addenda relating to these specifications on the City's website at www.bellevuewa.gov under "Departments", "Finance", "Bid Information" then "Current Bid Opportunities, RFP's and RFQ's". It is the vendor's responsibility to confirm as to whether any addenda have been issued.

2.03 Withdrawal of Proposal

Proposals may be withdrawn at any time prior to the submission time specified in Section 1.08, provided **notification is received in writing**. Proposals cannot be changed or withdrawn after the time designated for receipt.

2.04 Rejection of Proposals

The City reserves the right to reject any or all proposals, to waive any minor informalities or irregularities contained in any proposal, and to accept any proposal deemed to be in the best interest of the City.

2.05 Code of Conduct for Solicitations

Definitions:

Solicitations - method of acquiring goods, services, and construction for public use in which offers are made to the City between two or more sources. Typical documents used by the City are titled: Invitation to Bid, Invitation to Quote, Request for Proposals, Request for Qualifications Request for Information, or any other method of obtaining competitive offers.

Blackout Period - The period between the time a solicitation is issued by the City and the time the City awards the contract.

Lobbying - The attempt to persuade or influence any City employees, officials, or representatives responsible for reviewing, evaluating, ranking or awarding the work or contract for goods or services for or against any solicitation; provided, however, that lobbying shall not include the submission of required materials in direct response to the solicitation according to the instructions to respondents in such solicitation.

Conduct of Participants - After the issuance of any **solicitation**, all bidders, proposers, contractors, consultants or individuals acting on their behalf are hereby prohibited from **lobbying** any City employee, official or representative at any time during the **blackout period**.

Sanctions - The City may reject the submittal of any bidder, proposer, contractor and/or consultant who violates the policy set forth herein.

2.06 Proposal Modification and Clarifications

The City reserves the right to request that any vendor clarify its proposal or to supply any additional material deemed necessary to assist in the evaluation of the proposal.

Modification of a proposal already received will be considered only if the request is received prior to the submittal deadline. All modifications must be made in writing, executed and submitted in the same form and manner as the original proposal.

2.07 Proposal Validity Period

Submission of a proposal will signify the vendor's agreement that its proposal and the content thereof are valid for 180 days following the submission deadline unless otherwise agreed to in writing by both parties. The proposal will become part of the Contract that is negotiated between the City and the successful Vendor.

2.08 Proposal Signatures

- 1) An authorized representative must sign proposals, with the vendor's address, telephone and email information provided. Unsigned proposals will not be considered.
- 2) If the proposal is made by an individual, the name, mailing address and signature of the individual must be shown.
- 3) If the proposal is made by a firm or partnership, the name and mailing address of the firm or partnership and the signature of at least one of the general partners must be shown.
- 4) If the proposal is made by a corporation, the name and mailing address of the corporation and the signature and title of the person who signs on behalf of the corporation must be shown.
- 5) The City reserves the right to request documentation showing the authority of the individual signing the proposal to execute contracts on behalf of anyone, or any corporation, other than himself/herself. Refusal to provide such information upon request may cause the proposal to be rejected as non-responsive.

2.09 Public Records

Under Washington state law, the documents (including but not limited to written, printed, graphic, electronic, photographic or voice mail materials and/or transcriptions, recordings or reproductions thereof) submitted in response to this RFP (the "documents") become a public record upon submission to the City, subject to mandatory disclosure upon request by any person, unless the documents are exempted from public disclosure by a specific provision of law. If the City receives a request for inspection or copying of any such documents it will promptly notify the person submitting the documents to the City (by U.S. mail and by fax if the person has provided a fax number) and upon the written request of such person, received by the City within five (5) days of the mailing of such notice, will postpone disclosure of the documents for a reasonable period of time as permitted by law to enable such person to seek a court order prohibiting or conditioning the release of the documents. The City assumes no contractual obligation to enforce any exemption.

2.10 Business Registration and Taxation

The vendor awarded the Contract will be subject to City of Bellevue Business Registration and Business Taxation as presented in the Bellevue City Code. Questions about the City's Business and Occupation (B&O) tax should be directed to the City's Tax office at (425) 452-6851.

2.11 Non-Endorsement

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

2.12 Non-Collusion Certificate

The proposal submitted for this RFP shall include the **Non-Collusion Certificate (Attachment "A")**.

2.13 Insurance Requirements

The City will require the selected Vendor to comply with the **Insurance Requirements** listed in **Attachment "B"**.

2.14 Equal Opportunity & Title VI Requirements

The City is an equal opportunity employer and requires all Vendors to comply with policies and regulations defined in the **Equal Opportunity & Title VI Requirements defined in Attachment "C"**. The Vendor, in the performance of the Contract, agrees not to discriminate in its employment because of the employee's or applicant's race, religion, national origin, sexual orientation, ancestry, sex, age or physical handicap. The requirements of Bellevue City Code Section 4.28.143 entitled "Equal Opportunity" provided to the Vendor with the Request for Proposals, are hereby incorporated herein, and shall be binding on the vendor.

2.15 Non-Disclosure Agreement

The City will require the selected Vendor to comply with the **Non-Disclosure Agreement** listed in **Attachment "D"**. Selected vendor will be required to execute this agreement.

2.16 Technology Resource Usage Policy

The City will require the selected Vendor to comply with the Technology Resource Usage Policy (TRUP) listed in **Attachment "F"**.

2.17 Information Security Requirements

The City will require the selected Vendor to comply with the Information Security Requirements listed in **Attachment "G"**.

2.18 Other Compliance Requirements

In addition to nondiscrimination and affirmative action compliance requirements previously listed, the Vendor awarded the Contract shall comply with federal, state and local laws, statutes and ordinances relative to the execution of the work. This requirement includes, but is not limited to, protection of public and employee safety

and health; environmental protection; waste reduction and recycling; the protection of natural resources; permits; fees; taxes; and similar subjects.

2.19 Ownerships of Documents

Any reports, studies, conclusions and summaries prepared by the Vendor shall become the property of the City.

2.20 Cooperative Purchasing

RCW 39.34 allows cooperative purchasing between public agencies (political subdivision) in the State of Washington. Public agencies which have filed an Intergovernmental Cooperative Purchasing Agreement with the City of Bellevue and which are actively participating may purchase from City of Bellevue contracts. Only those public agencies who have complied with these requirements are eligible to use this contract.

The City of Bellevue does not accept any responsibility for purchase orders or contracts issued by other public agencies. The public agency accepts responsibility for compliance with any additional or varying laws and regulations governing purchase by or on behalf of the public agency in question. The City of Bellevue accepts no responsibility for the performance of any purchasing contract by the Vendor, and the City of Bellevue accepts no responsibility for payment of the purchase price for any public agency.

2.21 Confidentiality of Information

All information and data furnished to the Vendor by the City, and all other documents to which the Vendor's employees have access during the term of the Contract, shall be treated as confidential to the City. Any oral or written disclosure to unauthorized individuals is prohibited.

Section 3. Requested Services

3.01 Duration of Services

The term of the Contract with the selected Vendor shall be from the date of execution of the Contract to the completion of the work defined in the Scope of Work of the Purchase Agreement. Additionally, it is expected that a Software License Agreement and/or Maintenance Agreement will be signed in conjunction with this agreement.

3.02 Vendor Information

The forms referenced below must be submitted with the vendor's proposal. **Please mark with an N/A** those areas that do not apply to your proposal. **Do not leave any space blank.**

Proposal Form - Complete **Form #1**

Vendor Information Requirements – Complete **Form #2**

Client References - Complete **Form #3**

3.03 Performance Expectations

If the vendor has had a contract terminated for default during the past five (5) years, all such incidents must be described. "Termination for default" is defined as notice to stop performance due to the vendor's non-performance or poor performance, and the issue was either (a) not litigated; or (b) litigated and such litigation determined the vendor to be in default.

Submit full details of all terminations for default experienced by the vendor during the past five (5) years, including the other party's name, address and telephone number. Present the vendor's position on the matter. The City will evaluate the facts and may, at its sole discretion, reject the vendor's proposal if the facts discovered indicate that completion of a contract resulting from this RFP may be jeopardized by selection of the vendor.

If the vendor has experienced no such termination for default in the past five (5) years, so declare.

If the vendor has had a contract terminated for convenience, non-performance, non-allocation of funds or any other reason, which termination occurred before completion of the contract, during the past five (5) years, describe fully all such terminations, including the name, address and telephone number of the other contracting party.

3.04 Scalability

The initial purchase of cameras resulting from this RFP is based off of current needs within the City. Depending upon future needs, this contract may include additional purchases of cameras.

3.05 Cost Requirements

The City expects to enter into a unit price contract for this project, where price is based on a per camera license model. Please see **Attachment “E”** for pricing itemization. All prices are to be in U.S. dollars. All applicable taxes to be paid by the City must be separately shown. The vendor awarded the Contract will be subject to City of Bellevue business registration and business taxation as provide in Chapters 4.03 and 4.09 of the Bellevue City Code (for details call the City Tax office at 425-452-6851).

Vendors must itemize the unit and extended price for each product and service proposed as part of the proposed solution. Cost information must include all expected implementation and operating costs, both one-time and ongoing. Specific model numbers and capacities should be included. Information about license sizes must be provided. Vendors should describe and quote optional components (including query tools, report writers, etc.) as individual and separate items. Any upgrade to the base system needed for optional components must be included in the cost of those components (defined in **Attachment E - Pricing**).

In addition to the breakdown of costs described above, the City of Bellevue would like to have a quoted hourly rate for professional services that may be required to complete our project, but were not anticipated and included in this RFP. The quoted rate(s) is expected to be applied for the duration of the project (as described herein). They should include, but are not limited to: project management, programmer/analyst, and technical support analyst.

Payment Schedule: Please include a proposed payment schedule as outlined in **Attachment “E”**.

Section 4. Technical Architecture Requirements

This section documents the technical requirements for the Avigilon Control Center Enterprise edition solution and requests information from the vendor that is to be provided in accordance with the instructions contained in Section 1. All questions stated in this section are highlighted in **blue**.

4.01 Network

The City's data infrastructure is a managed TCP/IP network with Gigabit and 10Gb Ethernet Routed/Switched architecture connected via fiber between geographically dispersed buildings and remote locations. The City's redundant core network connects to multiple locations via privately owned fiber optic cable with dark fiber available to be used for this project, including pathway to the Bellevue Service Center (BSC). Database, application, enterprise, and web servers are located at City Hall with some redundant servers located at BSC.

4.02 Servers and Operating System

The City of Bellevue's Data Center has monitored physical access, a raised floor, and is a temperature and humidity controlled environment. The City runs 32-bit and 64-bit HP servers. The standard configuration includes rack mounted Hewlett-Packard Proliant servers with redundant power supplies connected to dual power distribution units, Smart Array SCSI controllers, Ultra 320 SCSI disk drives, and two built-in HP Ethernet 10/100/1000 network cards. Typically, three or more drives are configured as RAID5 and two drives are mirrored to act as the system drive in a RAID1 configuration.

City standards for the servers specify the operating system to be Microsoft Windows 2008, installed on the C partition, and all applications are restricted to residing on non-O/S disk partitions. All servers are currently backed up on a regular schedule using EMC Legato Networker software, and all servers have Symantec Antivirus clients installed.

Except for 4 cluster nodes, all servers utilize only one of the two built-in NICs. The file server is located on DFS shares on a unix based Netapp FAS 3140 SAN.

Server Solution

Please complete the following table to specify the **recommended** or optimal server configuration required to operate the Avigilon Control Center.

Operating system(s) with version number	
Recommended hard drive free space	
Recommended RAM	
Recommended processor and speed	

If there is any overriding reason to recommend a different operating system than Windows 2008 R2 standard for the database services layer of the proposed system, please explain.

4.03 Client Workstations

All client workstations will run City-provided antivirus software (System Center 2012 Endpoint Protection), as well as the Microsoft Systems Management Server client. All client workstations will be patched regularly according to City standards.

Client Solution

Please complete the following table to specify the **recommended** or optimal workstation configuration required to operate the Avigilon Control Center Client Solution.

Operating system(s) with version number	
Recommended Graphics	
Recommended RAM	
Recommended processor and speed	

Web Browser Solution

Please complete the following table to specify the **recommended** or optimal workstation configuration required to access the Avigilon Control Center solution using a PC with a web browser.

Operating system(s) with version number	
Recommended Graphics	
Recommended RAM	
Recommended processor and speed	
Recommended Web Browser and Version	

Mobile Device Solution

Please complete the following table to specify the **recommended** or optimal configuration required to access the Avigilon Control Center Mobile solution using a Mobile Device.

Operating system(s) with version number	
--	--

4.04 System Operation and Maintenance

4.04.01 Application Security

- Discuss your experience integrating Avigilon Control Center Enterprise Edition with Microsoft's Active Directory.
- The City of Bellevue will use group level security to provide access to the Avigilon Software. Describe your experience with this model.

4.04.02 Web Application Security

Please comment on each of the following Minimum Security Requirements for Web Applications (if applicable):

- HTTPS and SSL encryption may be required in some City of Bellevue sites.
- There must be authentication and session management to prevent attackers from compromising passwords, keys, session tokens, and any efforts to assume the identities of the other users.
- There must be proper error handling.
- There must be Input validation against Cross Site Scripting and SQL Injection attack.
- The website is expected to comply with the City's "Technology Resource Usage Policy" which is included as Attachment "F". Please comment on the compliance of your solution.

4.04.03 System Maintenance

Describe how you work with Avigilon regarding the product's ongoing maintenance.

Describe your preventative schedule for cameras if purchased through your company.

4.04.04 Support

- Is there an extended warranty to purchase? If so, describe what it includes.
- Describe your ongoing user support, including whether you provide a service call desk, procedures for handling different types of calls, ability to prioritize critical calls, and ability to respond to calls within a reasonable time period.
- The City prefers a response from the service desk serious calls (prevents the City from performing day-to-day tasks) within four hours and a response to critical calls (delay in work or loss of data due to system failure) within 1 hour. Provide validation of this capacity.
- The City allows vendors to support remotely using VPN. Confirm your ability to comply with City procedure for remote access.
- Do you provide on-site support if needed?

- Will you continue to provide support if upgrades are not implemented?
- Describe how problems and/or bugs are reported, fixes developed, and status tracked for the proposed system.
- Describe how you provide information from Avigilon to keep clients informed of outstanding problems and fixes for the proposed system.
- Describe the process to communicate with Avigilon for receiving, evaluating, and implementing requests for enhancements to the proposed system, after it is installed and in use.
- Identify any training program(s) that Avigilon offers to introduce users to software updates.

4.04.05 Support Staff Resources

Recommend a typical range of personnel resources needed to maintain the proposed system.

4.04.06 Licensing

Include a copy of Avigilon's software license agreement.

4.04.07 System Interfaces and Connectivity

- The Avigilon Control Center Enterprise Edition will interoperate with the City of Bellevue's Active Directory.
- Discuss the methods, tools, and documentation that you utilize to integrate the Avigilon Control Center Enterprise Edition with Windows Active Directory.

4.04.08 Upgrades

What is Avigilon's typical average upgrade schedule? Discuss your experience in supporting the upgrade schedule for the proposed system. Describe any upgrades anticipated within the next two years, including schedule and additional costs.

4.04.09 Data Storage

Describe the archiving capabilities of the Avigilon Control Center Enterprise edition system. Does the system provide user defined archiving selection criteria? Describe how archived data is accessed.

4.05 System Implementation

4.05.01 Project Implementation and Training Plan

The vendor shall include a typical timeline with this proposal including major milestones for tasks and subtasks, dates and both vendor and customer resources. **The required format for the**

timeline is MS Project format. The plan should adhere to any pertinent milestone dates in the RFP Schedule in Section 1.05.

Include a description of your overall approach to each of the following task areas (if applicable):

- System installation
- System configuration
- Training [A sample of training materials & documentation should be included]
- Test planning and execution
- System interface design and support
- System roll-out, procedures, and support

4.06 City of Bellevue Department Existing Setup

Transportation

- 4 Channel DVR from GE
- Axis (partner with WADOT)
- Cohu Netcam with Axis Web gui
- 42 Analog Cameras
- 12 Axis encoders in the field
- 48 Axis Blades in MEC02

Facilities

- 4 DVRs with 16 channels from Pelco
- Pelco DS Control Point and Integral clients
- 32 Analog cameras
- Planning expansion to Bellevue Service Center

Utilities

- 4-8 channel DVRs from Everfocus
- 28 sites, including secure facilities
- Ecor cameras (Analog) wth Pelco enclosure

Parks

- DVR
- 2 sites with 6 cameras at each
- Fiber cable to cameras – Highland Center
- Cat5 – Crossroads Community Center and Skate Park
- Plans to expand to other community centers

Information Technology

- DVR
- 10 Cameras (NOC and MEC)

Section 5. Scope of Services

The City matrices on the following pages identify the scope of service needs that the Vendor should meet when implementing the Avigilon Control Center Enterprise edition Server and Client Software. Vendors must provide an answer for every requirement. If the requirement does not pertain to the proposal being submitted "N/A" must be placed in the requirement.

Use this key to determine which code to place in each of the requirement matrices below.

Matrix Column	Description
Solution Functional Requirements	This column presents desired functionality, technical, and interface capability.
Code	<p>3 - Vendor can completely meet this requirement.</p> <p>2 - Vendor can meet requirement with some exceptions or modifications.</p> <p>1 - Vendor will not be able to meet requirement.</p>
Comments	<p>In this column, please provide any additional information about your responses.</p> <p><i>Although costs are requested in a separate section, please provide a realistic dollar estimate if there is additional cost associated with your solution.</i></p>

Services Requirements	Code	Comments or Additional Information
General Requirements		
Vendor must submit a signed and dated proof of authorization to sale and/or service manufacturer products.		
Vendor must submit signed and dated proof of open and active account with manufacturer products.		
Vendor must submit signed and dated proof of open line of credit with manufacturer products.		
Vendor must have at least five (5) years of experience installing the specified type of equipment.		
The vendor providing and installing the Avigilon Access Control Client Enterprise (ACC) software must be a certified partner for the products proposed as well as an authorized installer.		
Vendor must employ at least one individual who has achieved the appropriate Certification from Avigilon.		
Each employee from the vendor who will work onsite at City facilities, must pass a background check and finger print identification, to allow access to server rooms and access to secured facility locations.		
Vendor must have a response time that is within four (4) hours for Serious Calls (prevents City from performing day-to-day tasks), and within one (1) hour for Critical Calls (a critical software error), with the capability to be onsite within two (2) hours during regular operating hours..		
Provide a support response schedule, indicating distance from the main campus and the maximum time to respond via phone and the time to arrive at the various City of Bellevue facilities for support needs on a normal business day.		

Services Requirements	Code	Comments or Additional Information
Vendor must provide documentation of completed camera manufacturer training and certification.		
Vendor is responsible for any measurements, calculations, and other details for best recommendation of type and placement of cameras for each of the City's identified sites.		
<p>The Vendor shall work with Avigilon to conduct formal on-site training sessions. It shall be the responsibility of the Vendor to coordinate time and location of training sessions with the Owner. Provide documented general instructions as follows:</p> <ul style="list-style-type: none"> • Provide instruction to designated personnel to include the location, inspection, normal maintenance, testing, and operation of all system components. • Provide instruction to designated personnel on the functions and operation of the system provided including capabilities, limitations, and the meaning of status messages. State the proper procedure for testing, routine maintenance. Provide detailed instruction on the operation of the Avigilon Control Center system operation. 		
Detailed specification sheets of all equipment that would be required to implement the Avigilon software MUST be submitted with bid.		

Services Requirements	Code	Comments or Additional Information
<p>Vendor should describe the warranty and upgrade options provided in the solution. Responses are expected to provide specifications and recommendations for the following needs related to the proposed solution.</p> <ul style="list-style-type: none"> • The solution shall provide information related to warranties for ANY camera from ANY camera manufacturer utilized in the solution purchased through the Vendor. • The solution shall provide for System Software Maintenance Releases or “patches” on the purchased software version at no charge during warranty and/or service period. 		
<p>The vendor must quote a complete system including delivery, installation, startup, integration, implementation, training, warranty, and maintenance.</p>		
<p>The vendor must have experience configuring Avigilon Control Center Enterprise with Active Directory, to include various security group and user scenarios.</p>		
<p>The vendor shall make a thorough inspection and test of the complete installed system, to insure the following:</p> <ul style="list-style-type: none"> • A complete and functional system is delivered. • Security Camera System is installed in accordance with applicable codes, industry standards and manufacturer’s recommendations. 		
<p>The Vendor shall work with the City to test that each camera is located properly, aimed and focused for the intended coverage area, through the capabilities of Avigilon’s Control Center Enterprise Client. All camera views will be signed-off by the owner as acceptable.</p>		

Services Requirements	Code	Comments or Additional Information
Cost Requirements		
City of Bellevue will purchase the necessary Server Hardware, but will need recommendations for server storage and number of servers based on performance recommendation from Avigilon.		
Camera Licensing, provide a breakdown of best price based on Avigilon's per camera licensing method. Show individual camera, blocks of camera purchased. Provide cost to purchase and license Avigilon brand camera versus other camera maker.		
Cameras listing, of the preferred camera types available for Avigilon software and local availability/support from camera vendor, including a brief feature set for each one. Based on the types of facilities owned by the City of Bellevue (indoor public areas, secured areas, outdoor).		
If cameras are purchased through the Vendor, provide a typical installation cost for the cameras to include physical installation, camera focusing, and testing, as needed (please include what post installation support is included in this price).		
Price for support either by hour, day, or service contract with service level options, to include normal and off-business hours.		
Cost of Avigilon's mobile application license		

Section 6. Proposal Evaluation and Vendor Selection

6.01 Evaluation Procedures

Proposals will be evaluated by the Selection Committee. The Selection Committee will consider the completeness of a vendor's proposal and how well the proposal meets the needs of the City. In evaluating the proposals, the City will be using a criteria evaluation process. Evaluations will be based on criteria as outlined in Section 6.02. All proposals will be evaluated using the same criteria and possible points.

6.02 Scoring and Evaluation Factors

The evaluation factors reflect a wide range of considerations. While cost is important, other factors are also significant. Consequently, the City may select other than the lowest cost proposal. The objective is to choose the vendor capable of providing quality vendor services that will help the City achieve the goals and objectives of the requested services within a reasonable budget.

Evaluations will be based on criteria as defined below. All proposals will be evaluated using the same criteria and possible points.

Evaluation Criteria	Possible Points
Responsiveness/Completeness of Proposal (i.e., Were all the forms completed and everything included that was required by the RFP? Were explanations in Comments or Additional Information areas adequate?)	10
Experience/Qualifications (i.e., Vendor's experience working within the requested services arena; vendor's experience working with municipalities; vendor's ability to successfully complete the scope of services on time and on budget; vendor's ability to successfully work with City staff; vendor's references)	35
Scope of Services (i.e., Does the vendor understand what it will take to successfully achieve the goals and objectives of the requested services? Did the vendor propose any revisions and/or changes to the draft Scope of Services that would better serve the City?)	25
Budget (i.e., does the budget seem reasonable for the scope of services proposed; does the budget provide the City good value?)	30
Total Points Possible	100

6.03 Selection Process

After the proposals are evaluated, the Selection Committee will determine whether formal presentations (product demonstration) and interviews are necessary, and if so, which vendors from the 'short list' may be invited to make a formal presentation and/or sit for a panel interview with the Selection Committee. If The City chooses to require formal presentations, demo scripts will be sent to each of the invited 'short

list' vendors. The scripts are required to provide an objective tool for the scoring of the product demonstration.

At this time, The City may choose to contact officials from other jurisdictions regarding the vendor, their prior work experience and their ability to successfully complete the scope of services. The City may request clarification or additional information from a specific vendor in order to assist in the City's evaluation of the proposed solution.

Two finalists are typically announced and, at the City's option, invited back for follow up demonstrations and questions. The Selection Committee will then formulate their recommendation for award of the Contract.

6.04 Contract Award and Execution

The City reserves the right to make an award without further discussion of the proposal submitted. **Therefore, the proposal should be initially submitted on the most favorable terms the vendor can offer.**

The City may require changes in the scope of services as deemed necessary by the City, before execution of the Contract. The City shall not be bound or in any way obligated until both parties have executed a vendor contract.

The general conditions and specification of the RFP and the successful Vendor's response, as amended by Contract between the City and the successful Vendor, including e-mail or written correspondence relative to the RFP, will become part of the Contract documents. Additionally, the City will verify vendor representations that appear in the proposal. Failure of a vendor to perform services as represented or any misrepresentations may result in elimination of the vendor from further competition or in Contract cancellation or termination.

The vendor selected as the apparently successful Vendor will be expected to enter into a contract with the City. The City uses its standard Purchase Agreement, Software License Agreement and Software Maintenance Agreement templates. Those vendors qualifying as 'short list' vendors will receive these templates. The foregoing should not be interpreted to prohibit either party from proposing additional contract terms and conditions during negotiations of the final contract.

If the selected Vendor fails to sign the Contract within ten (10) business days of delivery of the final Contract, the City may elect to cancel the award and award the Contract to the next-highest ranked vendor.

No parties may incur any cost chargeable to the proposed contract before the date of execution of the Contract.

IP Camera and NVR Solution

Form #1 Proposal Form

Vendor Name	
Vendor Address	
City, State, Zip Code	
Telephone #	
Email Address	

1. Response:

In response to the City's Request for Proposal, we offer the following:

I. Cover Letter

Signed by vendor representative authorized to bind the proposing firm contractually.

II. Table of Contents

III. Executive Summary

A one-page high-level overview of the solution being proposed

IV. Responses to Form 2 - Vendor Information Requirements

A. Copy the requirement tables as they appear in Form #2.

B. Be sure to provide an answer to each requirement. If the requirement does not pertain to your proposal, enter "N/A" in the table. If there is no table, be sure to provide the documentation requested. **Leaving a requirement blank may deem the vendor unresponsive.**

C. The vendor requirements are:

- 1) Company Information
- 2) Financial and Credit References
- 3) Project Staff Information
- 4) **Form #3** Client References
- 5) Contract Performance (must declare, as defined in Section 3.03)

V. Responses to Section 4- Technical Architecture Requirements

- A. Copy the requirements as they appear in Section 4.
- B. Be sure to provide an answer to each requirement or question in all sections. If the requirement does not pertain to your proposal, answer the question with “Not Applicable” and be sure to provide the documentation requested. **Leaving a requirement blank may deem the vendor unresponsive.**

VI. Responses to Section 5 - Functional Requirements

- A. Copy the requirement tables as they appear in Section 5.
- B. Be sure to provide an answer to each requirement. If the requirement does not pertain to your proposal, enter “N/A” in the table. If there is no table, be sure to provide the documentation requested. **Leaving a requirement blank may deem the vendor unresponsive. You are encouraged to include comments and provide exhibits, as needed.**

VII. Attachments

Please provide the following as attachments to your proposal:

- A. Non-Collusion Certificate (Attachment A).
 - This certificate must be notarized.
- B. Insurance Requirements (Attachment B).
 - Please provide evidence of insurance in the required amounts.
- C. Equal Opportunity & Title VI Requirements (Attachment C).
 - Please complete and sign the Affidavit of Equal Opportunity Compliance form.
- D. Non-Disclosure Agreement (Attachment D).
 - Please complete and sign the Non-Disclosure Agreement.
- E. Pricing (Attachment E).
 - Please list price for your proposed solution.

2. Exceptions:

Except as noted below, the undersigned hereby agrees to comply with all the terms and conditions put forth in the City's Request for Proposal.

Signed: _____

Dated: _____

Title: _____

IP Camera and NVR Solution

Form #2 Vendor Information Requirements

Company Information

Question	Vendor Answer
Type of Proposal being submitted	In-House or ASP <i>(please circle one)</i>
Company Name	
Home Office Address	
Washington Business Address	
Website Address	
Name of Person to be contacted concerning the proposal Title Address Telephone Number Fax Number Email Address	
Name of parent company, if applicable Home Office Address Telephone Number Website Address	
Describe the parent company's relationship with the vendor	
Does the person signing the proposal have the authority to sign on behalf of the vendor?	
Names of companies that will share significant and substantive responsibilities with the vendor in performing the scope of services under the Contract	
Length of time in business	
Gross revenue for the prior fiscal year (in US dollars)	
Percentage of gross revenue generated by implementation and licensing or use of proposed software	
Total number of clients with the proposed solution installed or in use	

Question	Vendor Answer
Total number of clients with the proposed solution installed or in use serving a customer base greater than 30,000	
Total number of other WA City clients with the proposed solution installed or in use.	
Total number of employees	
Distribute your total number of employees into the following functional areas:	
Customer and software support	
Installation and training	
Product development	
Technical programming and customization	
Other professional services	
Sales, marketing, and administrative support	

National, Regional, & Local Office Information

Location of national office			
Location of regional office nearest to Bellevue, WA			
Location of local office nearest to Bellevue, WA			
Identify the number of personnel at each location that would provide support for the proposed software (add lines as necessary)			
Job Title	Location	# of Employees	

Project Staff Information

Please duplicate table below as necessary and complete the following table for each of the key project staff members (including subcontractors) who will be assisting the City with implementation and training:

Staff member name	
Position in the company	
Length of time in position	
Project position and responsibilities	
Hours dedicated to project onsite	
Hours dedicated to the project remotely	
Education	
Certifications	
Previous work experience	
Technical skills and qualifications for the project	
Experience installing proposed system: Client name Contact person and phone # r Client size (population or customers served) Project Position/responsibilities Start date Scheduled end date Actual end date	

Attach to this form, and label appropriately, documentation showing that the vendor is duly organized and validly existing as a corporation or partnership in good standing, and licensed to do business in the City. If the vendor is not licensed to do business in the City, then the vendor must provide a sworn statement that it will take all necessary actions to become so licensed if selected as the selected Vendor.

IP Camera and NVR Solution

Form #3 Client References

Please duplicate form and provide three (3) client references.

Client Name	
Contact Name	
Title	
Phone Number	
Email Address	
Type of Services Provided	
Services Provided Similar to the City's requirements?	<input type="checkbox"/> Yes – Explain similarities: <input type="checkbox"/> No – Explain differences:

Attachment "A"
NON-COLLUSION CERTIFICATE

STATE OF _____)

COUNTY OF _____)

The undersigned, being duly sworn, deposes and says that the person, firm, association, co-partnership or corporation herein named, has not, either directly or indirectly, entered into any agreement, participated in any collusion, or otherwise taken any action in restraint of free competition in the preparation and submission of a proposal to the City of Bellevue for consideration in the award of a contract on the improvement described as follows:

RFP #12289 - IP Camera and NVR Solution

(Name of Firm)

By: _____
(Authorized Signature)

Title: _____

Sworn to before me this _____ day of _____ 2012.

Notary Public

CORPORATE SEAL:

Attachment “B” INSURANCE REQUIREMENTS

The Contractor shall procure and maintain for the duration of this Agreement insurance against claims for injuries to persons or damages to property which may arise from or in connection with the performance of the work hereunder by the Contractor, his agents, representatives, employees or subcontractors. The cost of such insurance shall be paid by the Contractor. Insurance shall meet or exceed the following unless otherwise approved by the City.

A. Minimum Insurance

1. Commercial General Liability coverage with limits not less than \$1,000,000 per occurrence / \$2,000,000 annual aggregate.
2. Stop Gap/Employers Liability coverage with limits not less than \$1,000,000 per accident/disease,
3. Business Automobile Liability coverage with limits not less than \$1,000,000 per accident for any auto.
4. Workers' Compensation coverage as required by the Industrial Insurance Laws of the State of Washington.

B. Self-Insured Retentions

Self-insured retentions must be declared to and approved by the City.

C. Other Provisions

1. Commercial General Liability policies shall be endorsed to:
 - a. Include the City, its officials, employees and volunteers as additional insureds,
 - b. Provide that such insurance shall be primary as respects any insurance or self-insurance maintained by the City,
2. Contractor or its Insurance Agent/Broker shall notify the City of any cancellation, or reduction in coverage or limits, of any insurance within seven (7) days of receipt of insurers' notification to that effect.

D. Acceptability of Insurers

Insurance shall be placed with insurers with a rating acceptable to the City.

E. Verification of Coverage

Contractor shall furnish the City with certificates of insurance required by this clause. The certificates are to be received and approved by the City before work commences. The City reserves the right to require complete, certified copies of all required insurance policies at any time.

F. Subcontractors

Contractor shall require subcontractors to provide coverage which complies with the requirements stated herein.

****The following coverages may also be required under this contract depending on the specific scope of work:***

Consultant's Error's & Omissions or Professional Liability with limits not less than \$1,000,000 per claim and as an annual aggregate.

Employee Dishonesty coverage endorsed for third party fidelity coverage for the City or endorsed to cover Client Property with limits not less than \$1,000,000 per occurrence and as an annual aggregate.

Network Security & Privacy Liability coverage with limits not less than \$1,000,000 per occurrence and as an annual aggregate, which names the City, its officials, employees and volunteers as additional insureds. Said coverage shall be primary and non-contributory.

Attachment “C”

EQUAL OPPORTUNITY & TITLE VI REQUIREMENTS

General Instructions

Applications: The following materials pertain to the Equal Opportunity Requirements of the City of Bellevue as set forth in Chapter 4.28.143 of the Bellevue City Code. All contractors, subcontractors, consultants, vendors and suppliers who contract with the City in a total amount of thirty-five thousand or more within any given year must comply with these requirements.

Affidavit: Before being considered for a contract of the magnitude listed above, all contractors will be required to submit the “Affidavit of Equal Opportunity Compliance” as part of their proposal/qualifications or upon the request of the Procurement Services Division.

Compliance: The City of Bellevue reserves the right to randomly select contractors, subcontractors, consultants, vendors or suppliers to be audited for compliance of the requirements listed. During this audit, the contractors, etc. will be asked for a specific demonstration of compliance with the requirements.

Noncompliance: A finding of a noncompliance may be considered a breach of contract and suspension or termination of the contract may follow.

City contact: The City’s Compliance Office is the Procurement Services Division, and specific questions pertaining to this section may be directed to the Procurement Services Division at (425) 452-7876.

Bellevue City Code Excerpt

Section 4.28.143 of the Bellevue City Code establishes the requirements for all contractual service providers: “All contractors, subcontractors, consultants, vendors and suppliers who contract with the City of Bellevue in a total amount of thirty-five thousand or more within any given year are required to take affirmative action and comply with the following requirements of this section. There shall be included in any contract between such contractual services provider and the City of Bellevue the following provisions:

1. Contractor shall make specific and constant recruitment efforts with minority and women’s organizations, schools, and training institutions. This shall be done by notifying relevant minority and women’s organizations.
2. Contractor shall seek out eligible minority and women contractors to receive subcontract awards. Appropriate minority and women contractors shall be notified in writing of any bids advertised for subcontract work.
3. Contractor shall provide a written statement to all new employees and subcontractors indicating commitment as an equal opportunity employer and the steps taken to equal treatment of all persons.
4. Contractor shall actively consider for promotion and advancement available minorities and women.
5. Contractor is encouraged to make specific efforts to encourage present minority and women employees to help recruit qualified members of protected groups.
6. Contractor is encouraged to provide traditional and nontraditional employment opportunities to female and minority youth through after school and summer employment.
7. Contractor is encouraged to assist in developing the skills of minorities and women by providing or sponsoring training programs.

Willful disregard of the City’s nondiscrimination and affirmative action requirements shall be considered breach of contract and suspension or termination of all or part of the contract may follow.

All contractors, subcontractors, vendors, consultants or suppliers of the City required to take affirmative action must sign the affidavit of compliance and submit with the bid proposal or upon the request of the Purchasing Manager. All documents related to compliance steps listed above shall be presented upon the request of the Purchasing Manager. The Purchasing Manager shall serve as the compliance officer for the city and is authorized to develop and issue procedures for the administration of this section.”

Interpretations

In order to more readily determine compliance with BCC 4.28.143, the following interpretations are provided:

Requirement 1. When a contractor needs to recruit, they must notify minority and women’s organizations, schools and training institutions. Such “notification” can be in the form of an advertisement in newspapers or trade journals of general circulation in the metropolitan Seattle area.

When the contractor hires through a union hiring hall, the contractor must be able to provide confirmation, upon request by the City, that the hiring hall has an equal opportunity policy.

Requirement 2. When a contractor intends to subcontract out any work they shall notify minority and women contractors for the subcontract work. The requirements to notify minority and women contractors of any bids can be satisfied by advertising in newspapers or trade journals that are of general circulation in the metropolitan Seattle area.

Requirement 3. If and when a contractor hires new employees or contracts with subcontractors, the contractor must alert such employees and subcontractors to the contractor's commitment as an equal opportunity employer, etc. This requirement may be complied with by posting a notice of equal opportunity commitment at the job shack, or by the time clock.

Requirement 4. If and when a contractor promotes or advances employees, the contractor must consider all eligible employees. The City of Bellevue reserves the right to audit all contractors for compliance with the requirements set forth in BCC 4.28.143.

TITLE VI - NON-DISCRIMINATION IN FEDERALLY ASSISTED PROGRAMS:

SEC. 601. Assures that no person shall, on the ground of race, color, or national origin, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any program or activity receiving Federal financial assistance.

PART 1 – TITLE VI PROCEDURAL INFORMATION

1. **APPLICATIONS:** The following materials pertain to the regulations relative to nondiscrimination of Federally assisted programs of the Department of Transportation, Title 49, Code of Federal Regulations, part 21. Nondiscrimination assumes All Vendors, subcontractors, consultants, suppliers and manufacturers who contract with the City must Comply with these requirements.
2. **AFFIDAVIT:** Before being considered for a contract, all Vendors, etc. will be required to submit the Affidavit of Title VI Compliance as part of their proposal or upon request by the City's Procurement Services Division.
3. **COMPLIANCE:** The City of Bellevue reserves the right to randomly select Vendors, subcontractors, consultants, vendors or suppliers to be audited for compliance of the requirements listed. During this audit. The Vendors, etc. will be asked for a specific demonstration of compliance with the requirements.
4. **NON-COMPLIANCE:** A finding of non-compliance may be considered a breach of contract and suspension or termination of a contract may follow.
5. **CITY CONTACT:** The City's Compliance Officer is the Procurement Services Division, and specific questions pertaining to this section may be directed to the Procurement Services Division at (425) 452-7876.

PART 2 – ASSURANCES FOR CONSULTANTS, CONTRACTORS, SUBCONTRACTORS, SUPPLIERS AND MANUFACTURERS

1. **COMPLIANCE WITH REGULATIONS:** The Vendor shall comply with the Regulations relative to nondiscrimination in Federally assisted programs of the Department of Transportation (hereinafter DOT), Title 49, Code of Federal Regulations, part 21, as they may be amended from time to time, (hereinafter referred to as Regulations), which are herein incorporated by reference and made part of this contract.
2. **NONDISCRIMINATION:** The Vendor, with regard to the work performed during the contract, shall not discriminate on the grounds of race, color, sex, or national origin in the selection and retention of subcontractor, including procurement of materials and leases of equipment. The Vendor shall not participate either directly or indirectly in the discrimination prohibited by Section 21.5 of the Regulations, including employment practices when the contract covers a program, set forth in Appendix B of the Regulations.
3. **SOLICITATION FOR SUBCONTRACTORS, INCLUDING PROCUREMENT OF MATERIALS AND EQUIPMENT:** In all solicitations either by competitive bidding or negotiations made by the Vendor for the work to be performed under a subcontract, including procurement of materials or leases of equipment, each potential subcontractor or supplier shall be notified by the Vendor's obligations under this contract and the Regulations relative to the nondiscrimination on the ground of race, color, sex, or national origin.
4. **INFORMATION AND REPORTS:** The Vendor shall provide all information and reports required by the Regulations or directives issued pursuant thereto, and shall permit access to its books, records,

accounts, other sources of information, and its facilities as may be determined by the City of Bellevue or the Washington State Department of Transportation to be pertinent to ascertain compliance with such Regulations, orders and instructions. Where any information required of a Vendor is an exclusive possession of another who fails or refuses to furnish this information, the Vendor shall so certify to the City of Bellevue or the Washington State Department of Transportation as appropriate, and shall set forth what efforts it has made to obtain the information.

5. **SANCTIONS FOR NONCOMPLIANCES:** In the event of the Vendor's noncompliance with the nondiscrimination provisions of this contract, the City of Bellevue and the Washington State Department of Transportation shall impose such contract sanctions as it, or the Federal Highway Administration may determine to be appropriate, including, but not limited to:
 - a. Withholding of payments to the Vendor under the contract until Vendor complies, and/or;
 - b. Cancellation, termination, or suspension of the contract, in whole or in part.
6. **INCORPORATION OF PROVISIONS:** The Vendor shall include in provisions of paragraphs (1) through (6) in every subcontract, including procurement of materials and leases of equipment, unless exempt by the Regulations, or directives issued pursuant thereto. The Vendor shall take such action with respect to any subcontractor or procurement as the City of Bellevue or the U.S. Department of Transportation, Federal Highway Administration, may direct as a means of enforcing such provisions including sanctions for noncompliance. Provided, however, that in the event a Vendor becomes involved in, or is threatened with, litigation with a subcontractor or supplier as a result of such direction, the Vendor may request the City of Bellevue enter into such litigation to protect the interests of the City and, in addition, the Vendor may request the United States to enter into such litigation to protect the interests of the United States.

AFFIDAVIT OF EQUAL OPPORTUNITY & TITLE VI COMPLIANCE

_____ certifies that:
Respondent

1. If necessary to recruit additional employees, it has:
 - a. Notified relevant minority and women's organizations, or
 - b. Hired through a union hall with an equal opportunity policy.

2. It intends to use the following listed construction trades in the work under the contract:

3. In sourcing subcontract work for trades listed above, it has notified in writing appropriate minority and women contractors of bids for subcontract work.
4. It will obtain from its subcontractors and submit upon request, an Affidavit of Equal Opportunity Compliance as required by these bid documents.
5. It has provided a written statement to all new employees or subcontractors indicating its commitment as an equal opportunity employer.
6. It has considered all eligible employees for promotion or advancement when promotion or advancement opportunities have existed.

By: _____
(authorized signature)

Title: _____

Date: _____

Attachment “D”
CITY OF BELLEVUE NON-DISCLOSURE AGREEMENT
(STANDARD RECIPROCAL)

This Non-Disclosure Agreement (the "Agreement") is made and entered into as of the later of the two signature dates below by and between CITY OF BELLEVUE, a Municipal corporation (“COB”), and _____ corporation ("Company") and is entered into for _____. (what the project is about e.g. evaluation of the CIS system)

IN CONSIDERATION OF THE MUTUAL PROMISES AND COVENANTS CONTAINED IN THIS AGREEMENT AND THE MUTUAL DISCLOSURE OF CONFIDENTIAL INFORMATION, THE PARTIES HERETO AGREE AS FOLLOWS:

1. Definition of Confidential Information and Exclusions.

- (a) "Confidential Information" means nonpublic information that a party to this Agreement (“Disclosing Party”) designates as being confidential to the party that receives such information (“Receiving Party”) or which, under the circumstances surrounding disclosure ought to be treated as confidential by the Receiving Party. "Confidential Information" includes, without limitation, information in tangible or intangible form relating to and/or including released or unreleased Disclosing Party software or hardware products, the marketing or promotion of any Disclosing Party product, Disclosing Party's business policies or practices, and information received from others that Disclosing Party is obligated to treat as confidential. For purpose of this agreement, this confidential information also includes but is no limited to the following types of information, whether in writing or not: all documentation, other tangible or intangible discoveries, ideas, concepts, drawings, specifications, techniques, data or any other information including any information the Disclosing Party obtains from another party which the Disclosing Party treats as proprietary or designates as confidential information whether or not it is owned by the Disclosing Party. Except as otherwise indicated in this Agreement, the term “Disclosing Party” also includes all Affiliates of the Disclosing Party and, except as otherwise indicated, the term “Receiving Party” also includes all Affiliates of the Receiving Party. An “Affiliate” means any person, partnership, joint venture, corporation or other form of enterprise, domestic or foreign, including but not limited to subsidiaries, that directly or indirectly, controls, are controlled by, or are under common control with a party.
- (b) Confidential Information shall not include any information, however designated, that: (i) is or subsequently becomes publicly available without Receiving Party's breach of any obligation owed Disclosing Party; (ii) became known to Receiving Party prior to Disclosing Party’s disclosure of such information to Receiving Party pursuant to the terms of this Agreement; (iii) became known to Receiving Party from a source other than Disclosing Party other than by the breach of an obligation of confidentiality owed to Disclosing Party; (iv) is independently developed by Receiving Party.

2. Obligations Regarding Confidential Information

- (a) Receiving Party shall:
 - (i) Refrain from disclosing any Confidential Information of the Disclosing Party to third parties for two (2) years following the date that Disclosing Party first discloses such Confidential Information to Receiving Party, except as expressly provided in Sections 2(b) and 2(c) of this Agreement;
 - (ii) Take reasonable security precautions, at least as great as the precautions it takes to protect its own confidential information, but no less than prevailing standard of reasonable care in the Receiving Party’s industry, to keep confidential the Confidential Information of the Disclosing Party;

- (iii) Refrain from disclosing, reproducing, summarizing and/or distributing Confidential Information of the Disclosing Party except in pursuance of Receiving Party's business relationship with Disclosing Party, and only as otherwise provided hereunder; and
 - (iv) Refrain from reverse engineering, decompiling or disassembling any software code and/or pre-release hardware devices disclosed by Disclosing Party to Receiving Party under the terms of this Agreement, except as expressly permitted by applicable law.
- (b) Receiving Party may disclose Confidential Information of Disclosing Party in accordance with judicial action, federal or state public disclosure requirements, state or federal regulations, or other governmental order or requirement of law, provided that Receiving Party either (i) gives the undersigned Disclosing Party reasonable notice prior to such disclosure to allow Disclosing Party a reasonable opportunity to seek a protective order or equivalent, or (ii) obtains written assurance from the applicable judicial or governmental entity that it will afford the Confidential Information the highest level of protection afforded under applicable law or regulation. In the event the Disclosing Party elects to obtain a protective order or equivalent, or legally contest and avoid such disclosure, the Receiving Party shall fully cooperate with the Disclosing Party.
- (c) The undersigned Receiving Party may disclose Confidential Information only to Receiving Party's employees and consultants on a need-to-know basis. The undersigned Receiving Party will have executed or shall execute appropriate written agreements with third parties sufficient to enable Receiving Party to enforce all the provisions of this Agreement.
- (d) Receiving Party shall notify the undersigned Disclosing Party immediately upon discovery of any unauthorized use or disclosure of Confidential Information or any other breach of this Agreement by Receiving Party and its employees and consultants, and will cooperate with Disclosing Party in every reasonable way to help Disclosing Party regain possession of the Confidential Information and prevent its further unauthorized use or disclosure. Upon discovery of an inadvertent or accidental disclosure, the Receiving Party shall promptly notify the Submitting Party of such disclosure and shall take all reasonable steps to retrieve the disclosure and prevent further such disclosures. If the foregoing requirements are met, a Receiving Party shall not be liable for inadvertent disclosure.
- (e) The restrictions herein shall not apply with respect to Confidential Information which:
- (i) Is or becomes known to the general public without breach of this Agreement; or
 - (ii) Is or has been lawfully disclosed to a Receiving Party by a third party without an obligation of confidentiality;
 - (iii) Is independently developed by a Party without access to or use of the Confidential Information; or
 - (iv) At the end of the period of confidentiality set forth in this agreement.
- (f) All tangible information, including drawings, specifications and other information submitted hereunder, by the Receiving Party to the other shall remain the property of the Disclosing Party. The Receiving Party promptly shall return Confidential Information, including all originals, copies, reproductions and summaries of Confidential Information and all other tangible materials and devices provided to the Receiving Party, and shall cease any further use thereof, upon the first to occur of the following events:
- (i) written request of the Submitting Party;
 - (ii) termination of this Agreement; or
 - (iii) completion of the purpose for which the Confidential Information was disclosed. In lieu of the foregoing, the Receiving Party, upon mutual consent, may destroy all copies of the Confidential Information and certify to the Submitting Party in writing that it has done so.
- (g) The receiving Party shall not export, directly or indirectly, any Confidential Information or any products utilizing such data unless it first complies with any applicable laws and regulations pertaining thereto, including, but not limited to, U.S. export laws or traffic in arms regulations.

3. Remedies

The parties acknowledge that monetary damages may not be a sufficient remedy for unauthorized disclosure of Confidential Information and that Disclosing Party shall be entitled, without waiving any other rights or remedies, to such injunctive or equitable relief as may be deemed proper by a court of competent jurisdiction.

4. Miscellaneous

- (a) All Confidential Information is and shall remain the property of Disclosing Party. By disclosing Confidential Information to Receiving Party, Disclosing Party does not grant any express or implied right to Receiving Party to or under any patents, copyrights, trademarks, or trade secret information except as otherwise provided herein. Disclosing Party reserves without prejudice the ability to protect its rights under any such patents, copyrights, trademarks, or trade secrets except as otherwise provided herein. Except as expressly herein provided, no rights, licenses or relationships whatsoever are to be inferred or implied by the furnishing of Confidential Information specified above or pursuant to this Agreement.
- (b) The terms of confidentiality under this Agreement shall not be construed to limit either the Disclosing Party or the Receiving Party's right to independently develop or acquire products without use of the other party's Confidential Information. Further, the Receiving Party shall be free to use for any purpose the residuals resulting from access to or work with the Confidential Information of the Disclosing Party, provided that the Receiving Party shall not disclose the Confidential Information except as expressly permitted pursuant to the terms of this Agreement. The term "residuals" means information in intangible form, which is retained in memory by persons who have had access to the Confidential Information, including ideas, concepts, know-how or techniques contained therein. The Receiving Party shall not have any obligation to limit or restrict the assignment of such persons or to pay royalties for any work resulting from the use of residuals. However, this sub-paragraph shall not be deemed to grant to the Receiving Party a license under the Disclosing Party's copyrights or patents.
- (c) This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof. It shall not be modified except by a written agreement dated subsequent to the date of this Agreement and signed by both parties. None of the provisions of this Agreement shall be deemed to have been waived by any act or acquiescence on the part of Disclosing Party, the Receiving Party, their agents, or employees, but only by an instrument in writing signed by an authorized employee of Disclosing Party and the Receiving Party. No waiver of any provision of this Agreement shall constitute a waiver of any other provision(s) or of the same provision on another occasion.
- (d) If either Disclosing Party or the Receiving Party employs attorneys to enforce any rights arising out of or relating to this Agreement, the prevailing party shall be entitled to recover reasonable attorneys' fees and costs. This Agreement shall be construed and controlled by the laws of the State of Washington, and the parties further consent to exclusive jurisdiction and venue in the federal courts sitting in King County, Washington, unless no federal subject matter jurisdiction exists, in which case the parties consent to the exclusive jurisdiction and venue in the Superior Court of King County, Washington. Company waives all defenses of lack of personal jurisdiction and forum non-conveniens. Process may be served on either party in the manner authorized by applicable law or court rule.
- (e) This Agreement shall be binding upon and inure to the benefit of each party's respective successors and lawful assigns; provided, however, that neither party may assign this Agreement (whether by operation of law, sale of securities or assets, merger or otherwise), in whole or in part, without the prior written approval of the other party. Any attempted assignment in violation of this Section shall be void.
- (f) If any provision of this Agreement shall be held by a court of competent jurisdiction to be illegal, invalid or unenforceable, the remaining provisions shall remain in full force and effect.
- (g) Either party may terminate this Agreement with or without cause upon ninety- (90) days prior written notice to the other party. All sections of this Agreement relating to the rights and obligations of the parties concerning Confidential Information disclosed during the term of the Agreement shall survive any such termination.
- (h) This Agreement is not intended to constitute, create, give effect to, or otherwise recognize a joint venture, partnership or formal business entity of any kind and the rights and obligations of the Parties shall be limited to those expressly set forth herein. Any exchange of Confidential Information under this Agreement shall not be deemed as constituting any offer, acceptance, or promise of any further contract or amendment to any contract which may exist between the Parties. Nothing herein shall be construed as providing for the sharing of profits or losses arising out of the efforts of either or both Parties. Each

Party shall act as an independent contractor and not as an agent of the other for any purpose whatsoever and neither shall have any authority to bind the other. Moreover, this Agreement shall create no obligation by either Party to disclose any particular kind or quantity of information to the other.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement.

COMPANY: _____
Address: _____

CITY OF BELLEVUE
450 110th Avenue NE
Bellevue, WA 980009-9012

By: _____
Name: _____
Title: _____
Date: _____

By: _____
Name: _____
Title: _____
Date: _____

Attachment “E” PRICING

Please complete this attachment by indicating all costs associated with each product and/or service included in the proposal. Also include aggregate pricing if price advantages are available.

- 1. APPLICATION SOFTWARE MODULES (Please attach an itemized list of costs for each product;)**
- 2. HARDWARE & EQUIPMENT– if applicable (Please attach an itemized list of cost for each product)**
- 3. SYSTEM INSTALLATION AND SETUP**
- 4. CONFIGURATION**
- 5. PROJECT MANAGEMENT SERVICES**
- 6. IMPLEMENTATION PLANNING & ASSISTANCE**
- 7. TRAINING**
- 8. SERVICE LAYER/INTEROPERABILITY LAYER DEVELOPMENT**
- 9. ANNUAL MAINTENANCE AND SUPPORT**
- 10. TRAVEL AND EXPENSES**
- 11. HOURLY RATE FOR ADDITIONAL PROFESSIONAL SERVICES**
- 12. OTHER – please itemize**

Attachment “F”

TECHNOLOGY RESOURCE USAGE POLICY

(TRUP)

Executive Summary

This policy is designed to establish acceptable and appropriate use of computer and information systems, networks and other information technology resources at the City of Bellevue. The purpose of these policies is to safeguard and protect all technology resources from anything other than authorized and intended use. The main points to remember are:

1. The City provides network, communications systems, equipment and devices. (“technology resources”) to carry out legitimate City business. By using the City’s technology resources, an employee consents to disclosing the contents of any data files, information and communications created on, stored on, transmitted, received or exchanged via its network, communications systems, equipment or devices.
2. There is no right to privacy in the use of City technology resources. By using the City’s technology resources an employee consents to monitoring, recording, and reviewing the use of that technology resource.
3. Users are expected to act lawfully, ethically and professionally, and to exercise common sense. Actions that are embarrassing to explain to the public, City Council, City Manager or media should be avoided.
4. Users who are granted access to critical data are responsible for its protection.
5. Incidental use for personal needs is allowed as long as that activity does not interfere with City business or conflict with any City policy or work rule.
6. Use of technology in violation of this policy is subject to disciplinary action up to and including termination.

(Technology definitions provided in section 12)

1. Scope

- 1.1. The following policies define appropriate use of the City of Bellevue network, computers, mobile computing devices, smart phones, all related peripherals, software, electronic communications, and Internet access. They apply to the access of the City’s network and use of computing technology resources at any location, from any device, via wired or wireless connection. They apply to all users of City technology resources regardless of employment status. Access to all networks and related resources require that each user be familiar with these policies and associated work rules. The City of Bellevue authorizes the use of computing and network resources by City staff, contractors, volunteers and others to carry out legitimate City business. All users of City computing and network resources will do so in an ethical, legal, and responsible manner. All use of technology resources must be consistent with the intent and requirements of all City policies and work rules. Technology resources may not be used to facilitate operation of a personal business such as sale of cosmetics, consulting, etc.

2. Ownership of Data

- 2.1. The City owns all data, files, information, and communications created on, stored on, transmitted, received or exchanged via its network, communications systems, equipment and devices (including e-mail, voicemail, text messages and Internet usage logs even if such communications resides with a third party provider) and reserves the right to inspect and monitor any and all such communications at any time, for any business purpose and with or without notice to the employee. The City may conduct random and requested audits of employee accounts (including accounts with commercial or other third party

providers if used in the course of conducting City business) in order to ensure compliance with policies and requirements, to investigate suspicious activities that could be harmful to the organization, to assist Departments in evaluating performance issues and concerns, and to identify productivity or related issues that need additional educational focus within the City. Internet, e-mail, voicemail, text message communications and Internet usage logs may be subject to public disclosure and the rules of discovery in the event of a lawsuit. The City's Internet connection and usage is subject to monitoring at any time with or without notice to the employee. There is no right to privacy in the use of City technology resources.

3. Personal Use

- 3.1. Technology resources may be used for incidental personal needs as long as such use does not result in or subject the city to additional cost or liability, interfere with business, productivity or performance, pose additional risk to security, reliability or privacy, cause or tend to cause damage to the City's reputation or credibility, or conflict with the intent or requirements of any City policy or work rule. Incidental personal usage should generally conform to limits typically associated with personal phone calls. This document does not attempt to address every possible situation that may arise. Professional judgment, etiquette, and common sense should be exercised while using City technology resources. Please note that any data stored on City systems including but not limited to email, word documents, and photos may be subject to public disclosure requests.

4. Internet/Intranet Usage

- 4.1. This technology usage agreement outlines appropriate use of the Internet/Intranet. Usage should be focused on business-related tasks. Incidental personal use is allowed as discussed under this section, but there is no right to privacy in an employee's use of the Internet/Intranet. Employee Internet usage is monitored. Web Usage Reports are provided to Directors to help them monitor their staff's use of the Internet.
- 4.2. Use of the Internet, as with use of all technology resources, should conform to all City policies and work rules. Filtering software will be used by the City to preclude access to inappropriate web sites unless specific exemptions are granted as a requirement of work duties (e.g., police have the ability to access sites on criminal activity, weapons etc.). Attempts to alter or bypass filtering mechanisms are prohibited. When it is available BellevueConnectStaff should be used for wireless access. Staff using City equipment should not use BellevueConnect, BellevueConnectOutdoor or other outside wireless services to bypass web filtering and monitoring.
- 4.3. Except for City business related purposes, visiting or otherwise accessing the following types of sites is prohibited:
 - "adult" or sexually-oriented web sites
 - sites associated with hate crimes or violence
 - personal dating sites
 - gambling sites
 - sites that would create discomfort to a reasonable person in the workplace
- 4.4. The City recognizes that public Internet communications technologies (Web 2.0) are effective tools to promote community and government interaction and that employees want to participate in public communication via blogging, discussion forums, wikis, mashups, social networking, message boards, e-mail groups and other media that are now commonplace tools by which people share ideas and information.

However, since activities on public Internet communication sites are electronically associated with City network addresses and accounts that can be easily traced back to

the City of Bellevue, the following rules must be followed for participation on these interactive public Internet communication sites:

- a. When expressing staff's personal view, make it clear that it does not necessarily represent the views of the City of Bellevue. Opinions or views other than those reflective of City policy must contain the following disclaimer: "The content of this electronic communication does not necessarily reflect the official views of the elected officials or citizens of the City of Bellevue."
- b. Always protect the confidentiality, integrity, and availability of all critical information.
- c. Employees must not post any material that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful, or embarrassing to or of any other employee, person, and/or entity.
- d. To protect staff's privacy and the privacy of others, phone numbers or email addresses must not be included in the content body.
- e. Public Internet communications activity should contribute to staff's body of work as an employee of the City and must not interfere with or diminish productivity.

5. E-Mail Usage

- 5.1. E-mail content must be consistent with the same standards as expected in any other form of written (or verbal) communication occurring in a business setting where documents are subject to public disclosure.
- 5.2. Users must manage their e-mail in accordance with records retention policies and procedures as defined and identified by the City Clerk's Office.
- 5.3. Use of the "Everyone_COB" or "Everyone_Staff" distribution lists is restricted to the City Manager's Office, Department Directors and their specific designees. Under no circumstances should an employee "Reply to All" to an Everyone_COB or Everyone_Staff message.
- 5.4. External mass distribution e-mails to 50 or more recipients are prohibited from City e-mail accounts. Staff communicating to distribution lists of 50 or more recipients should utilize GovDelivery "E-Mail Alerts," (which allow people to sign up to receive e-mails whenever substantive changes are made to city web pages) or listserv technology.
- 5.5. The City provides staff access to and support of the Exchange/Outlook messaging (e-mail) system. Access or usage of any other messaging systems is not allowed unless it is web based. Subject to the personal use limitations explained above, staff may access web-based personal email but should not download personal documents or attachments from these sites. Staff may not install client based software such as AOL for internet service on city equipment.
- 5.6. Users should be attentive to emails that have unusual or questionable subject lines to mitigate spam, phishing and script born viruses that come into the network through email attachments or by clicking on links that lead to hostile web sites. If you suspect phishing or script born viruses in email attachments immediately contact the support desk.
- 5.7. The use of e-mail to send or solicit the receipt of inappropriate content such as sexually oriented materials, hate mail, content that a reasonable person would view as obscene, harassing or threatening and having no legitimate or lawful purpose or contents falling within the inappropriate categories for internet usage is prohibited.
- 5.8. The incidental personal use of e-mail from a City account to express opinions or views other than those reflective of City policy must contain the following disclaimer: "The contents of this electronic mail message do not necessarily reflect the official views of the elected officials or citizens of the City of Bellevue."

6. Security

- 6.1. ITD must authorize all access to central computer systems. Each user is responsible for establishing and maintaining a password that meets City requirements as described in the City's password policy. The use of another user's account or attempt to capture other users' passwords is prohibited. Each user is responsible for restricting unauthorized access to the network by locking their computer or logging out of their computer account when leaving their computer unattended. Staff who discovers unauthorized use of their accounts must immediately report it to IT Support at support@bellevuewa.gov or call x2886.
- 6.2. The City of Bellevue will take the necessary steps to protect the confidentiality, integrity, and availability of all of its critical information. Critical information is defined as information which if released could damage the City financially; put employees at risk; put facilities at risk; or could cause legal liability. Examples of critical data include: employee health information, social security numbers, credit card holder information, banking information, police crime investigation information, etc.
- 6.3. Staff with access to critical information are responsible for its protection. Staff must take reasonable steps to ensure the safety of critical information including: avoid putting critical data on laptops; encrypting data any time it is electronically transported outside the City network; not storing, saving, or transmitting critical data to a home computer or other external computer; ensuring inadvertent viewing of information does not take place, and destroying or rendering the information unreadable when done with it.
- 6.4. Staff should not transport critical City data on unencrypted devices such as thumb drives, CD's, or Smartphones. The City has standards for encrypted USB drives that should be used for this purpose. Information about these standards can be obtained from ITD Support at support@bellevuewa.gov or call x2886.
- 6.5. Department ITGC representative approval is required prior to moving any and all physical media containing critical data (as defined in the City's Data Classification Policy) from a secured area.
- 6.6. The City will restrict access to critical information only to staff who have a legitimate business need-to-know. Each system owner is responsible for keeping an inventory of critical information and ensuring that access to it is limited.
- 6.7. Staff will be assigned unique user IDs and passwords for network access. Access to systems and applications containing critical information will only be allowed via unique user IDs. Access will be monitored and actions will be traceable to authorized users.
- 6.8. Staff are prohibited from sharing their passwords or allowing anyone else to use their network account for any reason.

7. Network Access and Usage

- 7.1. The Information Technology Department (ITD) must approve connecting devices to the City's network. This includes PCs, network hubs and switches, printers, handhelds, scanners, remote connections, and wireless or wired devices. The use of personal routers and wireless access points on the City network is not allowed.
- 7.2. The installation, removal, or altering of any software on City-owned equipment is prohibited without authorization from a department manager or designee.
- 7.3. Smart phones (Internet and/or e-mail capable cell phones) must meet and adhere to the current standards for those devices as established by ITD. Personally owned smart phones may be connected to the City's network after ITD approval. This approval will only be granted after verification that the phone meets City standards and staff have signed applicable smart phone and/or stipend agreements per the smart phone policy.

- 7.4. Exploiting or attempting to exploit any vulnerability in any application or network security is prohibited. Sharing of internal information with others that facilitates their exploitation of a vulnerability in any application or network security is also prohibited. It is also prohibited to knowingly propagate any kind of spyware, and/or denial of service attack or virus onto the City network or computers. Staff who encounter or observe vulnerability in any application or network security must immediately report it to IT Support at support@bellevuewa.gov or call x2886.
- 7.5. Staff must follow the privacy and rules governing the use of any information accessible through the network, even if that information is not securely protected.
- 7.6. Non-City staff (e.g. vendors, contractors) are required to have their personal computers (PC) scanned by ITD for virus detection prior to connecting to the City's network. If the PC is going to continue to be connected (even occasionally) to the City's network it must be scanned a minimum of every 30 days. Representatives of the contracting departments are responsible for assisting their contractors to engage ITD to perform these services by contacting ITD Support at support@bellevuewa.gov or calling x2886.
- 7.7. Disabling, altering, over-riding, or turning off any mechanism put in place for the protection of the network and workstation environments is strictly forbidden. This includes the installation of any software designed to circumvent security measures.
- 7.8. Because of band-width limitations inherent in any network system, use of the City's network to download non-business related information is prohibited. Examples include streaming video of baseball games, streaming audio of radio programs, MP3 files, on-line games, etc.
- 7.9. Transmission, distribution, or storage of any information or materials in violation of federal, state or municipal law is prohibited. Software that is copyrighted or licensed may not be shared or illegally distributed. Copyright violations are federal offenses that may result in civil and criminal penalties to employees and the City of Bellevue.
- 7.10. Users must manage their electronic documents in accordance with records retention policies and procedures as defined and identified by the City Clerk's Office. Documents past their retention schedules should be deleted from the network to save space and eliminate the need to backup unnecessary files.
- 7.11. Access to the City's network via VPN requires approval from ITD. VPN accounts will be audited quarterly. Accounts not actively being used will be deactivated or removed. Reactivation of intermittently used VPN accounts for vendor support purposes will be accommodated upon request. VPN users must have commercial up-to-date anti-virus software. Vendors accessing the City network via VPN must adhere to the rules in the Vendor VPN Access SOP
- 7.12. Remote access to the City's applications via Citrix requires approval from the employee's manager or supervisor.
- 7.13. At least annually, departments need to review and approve network accounts and accounts for their applications. ITD will assist as needed in doing these reviews.

8. Administration, Reporting and Violations/Discipline

- 8.1. Each Department will designate specific employees who have the authority to authorize ITD to provide accounts and access to technology resources. Suspected violations or concerns should be reported to IT Support at support@bellevuewa.gov or by calling x2886.
- 8.2. ITD, the Departments, and HR share responsibilities in enforcing the Technology Resource Usage Policy (TRUP) as follows

9. ITD Responsibilities

- 9.1. ITD is responsible for recommending TRUP guidelines that are enforceable.
- 9.2. ITD is responsible for enterprise monitoring of technology resources using security and monitoring tools. Security and monitoring information will be provided to HR as requested to support the investigation of TRUP or other policy violations.
- 9.3. If, in the normal course of business activities, ITD discovers violations of the TRUP, ITD will report the activities to the employee's supervisor, Director of HR, and/or to the City Manager depending upon the severity of the infraction.

10. Departments Responsibilities

- 10.1. Departments assist in the development and adoption of the TRUP through ITGC.
- 10.2. If, in the course of normal business activities, department management suspects an employee has or is violating the TRUP they must report the suspected infractions to Human Resources.
- 10.3. Departments are responsible for carrying out any disciplinary actions in response to TRUP violations.
- 10.4. Assist in education and communication on an ongoing basis

11. Human Resources Responsibilities

- 11.1. Human Resources assists in the development and adoption of the TRUP through ITGC.
- 11.2. Human Resources is responsible for integrating the TRUP into new hire orientation and training and ongoing training of City work rules and policies.
- 11.3. Human Resources is responsible for the evaluation of reported TRUP infractions, and may request additional monitoring information (e.g., security logs) from ITD as part of their investigation and evaluation process
- 11.4. Human resources is responsible for providing necessary information to Department Directors to facilitate and coordinate with department management the consistent application of disciplinary action when TRUP infractions occur.
- 11.5. As with any set of policies or rules, exceptions may be granted and documented on a case-by-case basis. These require authorization from the Department involved as well as from ITD. Some exceptions may also require City Manager approval.
- 11.6. Violations of the TRUP, work rules, or otherwise inappropriate use of technology resources are subject to disciplinary action up to and including termination. Actions that demonstrate a clear disregard for these policies and requirements and either resulted or could have resulted in damage or serious disruption to the City's network, systems, services, or data; or either resulted or could have resulted in damage to the City's credibility or reputation with the public may result in immediate discharge.

12. Definitions: (Courtesy of WebOpida.com and WikiPedia.com)

- 12.1. Blog - Short for Web log, a Blog is a Web page that serves as a publicly accessible personal journal for an individual. Typically updated daily, blogs often reflect the personality of the author. Blogging is when one posts to a Blog.
- 12.2. Incidental use – The use of City systems for limited personal use such as Internet browsing to look for and order personal items. This use should be limited to personal time such as lunch and breaks.
- 12.3. Mashup - a Web page or application that uses and combines data, presentation or functionality from two or more sources to create new services.
- 12.4. Media – see Physical Media
- 12.5. Phishing - The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information

that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user's information.

12.6. Physical Media – Media which is utilized to store data and could potentially be used to transport information out of secure areas. These include but are not limited to paper reports, faxes, thumb drives, and CDs.

12.7. Spyware - Any software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Spyware applications are typically bundled as a hidden component of freeware or shareware programs that can be downloaded from the Internet; however, it should be noted that the majority of shareware and freeware applications do not come with Spyware. Once installed, the Spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.

Spyware is similar to a Trojan horse in that users unwittingly install the product when they install something else. A common way to become a victim of Spyware is to download certain peer-to-peer file swapping products that are available today.

12.8. VPN – Short for virtual private network, a network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. VPN is used by outside computers to connect to the City of Bellevue network.

\\\\\\

Attachment “G”

INFORMATION SECURITY REQUIREMENTS

Consultants with access to City data or systems shall provide their services in a manner consistent with the City’s Information Security policies. This includes, but is not limited to, ensuring that user accounts are known only by the individual assigned access, and not shared with anyone unless approved by the City in advance. If Consultants have remote access into systems with City data, Consultants shall ensure that the remote access is conducted from IT systems which have the latest security patches, anti-virus, and malware signatures.

Consultants are required to protect City data per the following table:

Critical	<p>The most private and restricted type of data stored, processed or transmitted by the City (e.g. credit card data, individually identifiable health information, social security numbers). This type of data must be strictly monitored and controlled at all times.</p> <p>When in electronic form, such data must be stored and transmitted in encrypted form. The data also must be version controlled, and must not be sent or taken outside of the City without explicit permission of a City department manager or the data owner. Such data must only be sent to business partners who have executed an approved non-disclosure agreement (NDA) with the City.</p> <p>Unauthorized disclosure or use of such data would violate laws, regulations or standards and/or cause a significant adverse impact to the City, its citizens, or business partners.</p>
Confidential	<p>Data that is private and restricted (e.g. detailed information about the City’s security controls or computer network, citizen account information, employee performance reviews). This includes data which by statute is specifically exempted from public disclosure.</p> <p>Such data must be restricted to those having a need for specific access in order to accomplish a legitimate task.</p> <p>When in electronic form, such data may be stored and transmitted in encrypted form. The data must not be sent or taken outside of the City without explicit permission of a City department manager or the data owner. Such data must only be sent to business partners who have executed an approved non-disclosure agreement (NDA) with the City.</p> <p>Unauthorized disclosure or use of such data may violate laws, regulations or standards and/or would likely cause a significant adverse impact to the City, its citizens, or business partners.</p>

A Contractor responsible for providing managed hosting services (such as hosting a website on behalf of the City), the Contractor shall ensure that website, access control systems, and supporting Operating Systems and Applications are secure. At a minimum, this includes an annual review of all users with access to the systems, applications, and code provided by Contractor, an annual independent security assessment which includes vulnerability scans, network and application layer penetration tests, code reviews. Independent shall mean that the persons conducting the security assessment will be independent of the design, installation, or maintenance of the systems. Contractor shall have a centralized logging, monitoring, and alerting systems in place such as an Intrusion Detection System

(IDS) or Log Management Server. All systems which store, process, or transmit City data shall have updated anti-virus and updated security patches for all software that is no later than 30 days old.

These requirements are not substitutes for the Contractor's obligations under applicable regulatory requirements including, but not limited to, the Payment Card Industry (PCI), Criminal Justice Information System (CJIS), the Health Insurance Portability and Accountability Act (HIPAA), or State Laws. If Contractor has access or retains data that is considered critical or confidential by the City, Contractor acknowledges that it will properly turn over or destroy all data upon termination of the contract. Contractor agrees at reasonable times to provide to the City or to its assignees, the audit rights for all physical locations, systems or networks that store, process, or transmit data on behalf of the City, and will provide access to the independent security assessments within one (1) business day. Contractor shall provide prompt notice to the City of any confirmed or suspected security breach affecting the City's data or informational infrastructure that supports the City's contracted services. Prompt notice shall mean within four (4) hours of discovery of the confirmed breach. Notice will be provided by e-mail and telephone to City's primary technical contact and primary business contact.