

AMENDMENT #3

Human Resource Portal

July 1, 2009


The eCityGov Alliance and the City of Redmond, having entered an Agreement for NWProperty.net service dated June 21, 2004, now, in consideration of the mutual promises herein stated, the parties request amendment of the Agreement as follows:

1. **Human Resource Portal; GovJobsToday.com and Compensation and Classification** service Appendix G shall replace Appendix F and be added to this Agreement.

All other terms and conditions shall remain the same.

In witness whereof, the Parties have executed this Amendment as of the Effective Date.

eCityGov Alliance


Accepted By (Signature)

John Backman
Executive Director

Date: *7/27/09*

City of Redmond


Accepted By (Signature)

John Marchione
Mayor

Date:

Approved as to Form (Signature):

Attorney

Date:

AMENDMENT #3

Human Resource Portal

July 1, 2009

The eCityGov Alliance and the City of Redmond, having entered an Agreement for NWProperty.net service dated June 21, 2004, now, in consideration of the mutual promises herein stated, the parties request amendment of the Agreement as follows:

1. **Human Resource Portal; GovJobsToday.com and Compensation and Classification** service Appendix G shall replace Appendix F and be added to this Agreement.

All other terms and conditions shall remain the same.

In witness whereof, the Parties have executed this Amendment as of the Effective Date.

eCityGov Alliance

City of Redmond



 Accepted By (Signature)

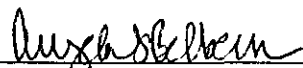
 Accepted By (Signature)

John Backman
Executive Director

John Marchione
Mayor

Date: **7/27/09**

Date:



 Approved as to Form (Signature):

Attorney **Angela S. Beibeck**

Date: **8/6/09**

APPENDIX G

Description of Application Service(s)

City of Redmond

I PRODUCT SUBSCRIPTION(S):

1. Regional Human Resource Portal - GovJobsToday.com including Compensation & Classification portal

II ANNUAL FEE(S)

2. **Annual Fee** – The pro-rata 2009 subscription fee is \$4,500¹. The anticipated 2010 annual fee is \$7,000, unless modified as provided in Section II. Annual Fee(s), paragraph 2, Establishment of Fees.
3. **Establishment of Fees** – Each year the Board shall set Subscriber Fees for the next calendar year, no later than September 30th. At such time the Board may increase, decrease or leave fees unchanged depending need.

III DESCRIPTION OF PRODUCT SERVICE: HUMAN RESOURCE PORTAL

4. The Human Resource Portal (Compensation & Classification) application functionality includes, but is not limited to:
 - (a) Secure user access
 - (b) Document Library folders including, but not limited to:
 - (i) Classification/Job Descriptions
 - (ii) Salary Schedules
 - (iii) Organizational Charts
 - (iv) Labour Agreements
 - (v) Benefits Information
 - (vi) Completed Salary Surveys
 - (vii) Miscellaneous
 - (c) Project team documents and communications

¹ The City of Redmond has paid the 2009 annual fee for the Compensation and Classification portal, leaving a 2009 balance for GovJobsToday.com of \$3,000.

5. The Human Resource Portal (GovJobsToday.com) application functionality includes, but is not limited to:
 - (a) Paperless recruitment
 - (i) Secure control of staff access (roles) to system with three levels of permissions
 - (ii) Job announcement posting to both GovJobsToday.com and the agency web site(s)
 - (iii) Track applicants by step/hurdle
 - (iv) Recruitment dashboard, track time-to-fill
 - (v) Clone a previous job announcement
 - (vi) Include predefined questions
 - (vii) Create new job specific questions on the fly
 - (viii) Candidate data is searchable
 - (ix) Quickly e-mail candidate application/resume
 - (x) Quickly e-mail candidate application/resume
 - (b) Data Management and Reporting
 - (i) Ability to export
 - (ii) Full EEO reporting
 - (iii) Quickly generate reports by date or job number
 - (iv) Filter data by: race count, gender count, EEO category, department, employment type, recruitment length, or recruitment count
 - (v) Transfer new hire information into your existing Human Resources Information System using a simple export feature
 - (c) Applicant profile
 - (i) Login
 - (ii) Edit
 - (iii) View job status
 - (d) Project team documents and communications

IV TECHNICAL DATA SPECIFICATIONS

1. Data supplied by the Subscriber

GovJobsToday.com job postings are solely the responsibility of Subscriber agency designated manager(s) and staff.
2. Data interfaced from the Alliance Application to the Subscribers back-end system

Not applicable

V SPECIAL REQUIREMENTS AND CONDITIONS

1. Restricted data policy: GovJobsToday.com
 - (a) It is the policy of the Alliance that member agencies shall not post or request GovJobsToday.com applicants to submit certain personally identifiable information, including, but not limited to:
 - (i) Date of birth
 - (ii) High school graduation date or year
 - (iii) Social security number
 - (iv) Drivers license number

Personally identifiable data of this nature shall be provided directly by the applicant to the authorized staff of the subscriber agency.
2. Subscriber agencies are responsible for the maintenance of:
 - (a) The content of relating to city/agency specific information such as contacts, address, phone numbers, email addresses and/or linked content.
 - (b) Actively participating in the application business team meetings.
3. Subscriber agency staff that desire user account(s), must;
 - (a) Be authorized by their agency
 - (b) Agree to the most current version of the Alliance Technology Resource Usage Policy

TECHNOLOGY RESOURCE USAGE POLICY

eCityGov Alliance Member Agencies

This policy is designed to establish acceptable and appropriate use of eCityGov Alliance computer and information systems, networks and other information technology resources accessed and used by member agency users. 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 Alliance provides computing and application resources ('technology') to carry out legitimate government business for member governments and agencies.
2. There is no right to privacy in the use of Alliance technology resources by agency users.
3. Personally identifiable information regarding individual users of the public application services provided by the Alliance is not collected, unless the user specifically volunteers such information as part of a desired transaction or service.
4. Agency users are expected to act lawfully, ethically and professionally, and to exercise common sense. Actions that are embarrassing to explain to the public, Executive Board, Executive Director or media should be avoided.
5. Agency users granted access to critical data are responsible for its protection.
6. Incidental use of Alliance business applications and/or systems by agency users for personal needs not is permitted, except users may access and make use of the publicly available Alliance web services for business and personal needs.
7. Use of technology in violation of this policy is subject to disciplinary action as determined by the employee's agency.

1. Definitions:

Alliance means eCityGov Alliance, an interlocal government agency

Host means the eCityGov Alliance technology and infrastructure host agency. Currently the Alliance host is the City of Bellevue.

Employee means Alliance member Agency employees, and contractors and/or volunteers contracted by the Alliance. *In addition to the Alliance Technology Usage Policy, City of Bellevue employees must adhere to the City of Bellevue Technology Usage Policy.*

Agency User means the employees, contractors, agents and/or volunteers of Alliance member cities, counties, other government agencies and non-government agencies.

Agency means the Alliance subscriber or partner member cities, counties, other government agencies and non-government agencies.

User means any user that accesses the publicly available services provided by the Alliance.

2. Scope

The following policies define appropriate use of the Alliance network, computers, all related peripherals, software, electronic communications, and Internet access. They apply to the access of the Alliance's network and use of computing technology resources at any location, from any device, via wired or wireless connection. They apply to all agency users of Alliance technology resources regardless of employment status. Access to all networks and related resources require that each agency user be familiar with these policies. The Alliance authorizes the use of computing and network resources by authorized agency staff, contractors, volunteers and others to carry out legitimate Alliance business. All agency users of Alliance 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 Alliance policies and work rules. Technology resources may not be used to facilitate operation of a personal business.

3. Ownership of Data

The Alliance and/or member agencies own all data stored on its network and systems (including e-mail, voicemail and Internet usage logs) 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 or agency user. The Alliance may conduct random and requested audits of employee and agency user accounts in order to ensure compliance with policies and requirements, to investigate suspicious activities that could be harmful to the organization, to assist agencies in evaluating performance issues and concerns, and to identify productivity or related issues that need additional educational focus within the Alliance. Internet and e-mail communications may be subject to public disclosure and the rules of discovery in the event of a lawsuit. The Alliance's Internet connection and usage is subject to monitoring at any time with or without notice to the employee or agency user. There is no right to privacy in the use of Alliance technology resources.

4. Personal Use

Alliance technology resources may not be used by employees or agency users for incidental personal except users may access and make use of the publicly available Alliance web services for business and personal needs when such personal use does not result in or subject the Alliance 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 Alliance's reputation or credibility, or conflict with the intent or requirements of any Alliance policy.

Important note: Personal use of agency business technology resources (computers, networks, Internet) is governed by the technology resource policy of each member agency.

5. Security

- a. The Alliance in conjunction with the host agency IT staff must authorize all access to Alliance applications. Each user is responsible for establishing and maintaining a strong password. The use of another person's account or attempt to capture other users' passwords is prohibited. Each agency 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. If an agency user discovers unauthorized use of your account, immediately report the incident to an Alliance employee.
- b. The Alliance 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 Alliance financially; put staff 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, and police crime investigation information.
- c. Agency users with access to critical information are responsible for its protection. Agency users must take reasonable steps to ensure the safety of critical information including: encrypting data any time it is electronically transported outside the Alliance network; ensuring that inadvertent viewing of information does not take place, and destroying or rendering the information unreadable when done with it.
- d. The Alliance will restrict access to critical information only to agency users who have a legitimate business need-to-know.
- e. Agency users 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 Agency users IDs. Access will be monitored and actions will be traceable to authorized Agency users.
- f. Agency users shall not share their password with any other person.

6. Network Access and Usage

- a. Exploiting or attempting to exploit into any vulnerability in any Alliance 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, denial of service attack, or virus onto the Alliance applications, network or computers. If Agency users encounter or observe vulnerability in any application or network security, they are report such activity to an Alliance employee immediately.
- b. Obey the privacy and rules governing the use of any information accessible through Alliance application(s), even if that information is not securely protected.

- c. Disabling, altering, over-riding, turning off any mechanism put in place for the protection of Alliance application(s) is strictly forbidden.
- d. 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 agency users and the Alliance.
- e. Agency users of Alliance application(s) in violation of this policy or otherwise inappropriate usage and is subject to disciplinary actions determined by his or her employing agency.

7. Alliance Responsibilities

- a. The Alliance is responsible for monitoring of use of Alliance application(s) using security and monitoring tools. Security and monitoring information will be provided to the Director of Human Resources of a member agency as requested to support the investigation of technology usage policy infractions.
- b. If, in the normal course of business activities, the Alliance discovers violations of the Technology Usage Policy, the Alliance will report the activities to Director of Human Resources of the member agency.
- c. The Alliance reserves the right to terminate access of any agency user to Alliance services and applications found to be in violation of the Alliance Technology Usage Policy.