ON-SITE AND REMOTE ACCESS CONFIDENTIALITY POLICY

The City of Rockville network ("Network") is comprised of all City information technology systems including, but not limited to network configuration, firewall configuration, host/server configuration, username/password pairs, access codes, any and all data contained on computers owned, operated, or maintained by the City of Rockville ("City"). This includes City owned personal laptop/PC computers and/or Contractor owned laptops/PCs if City data is stored on these systems.

Contractor may, in the course of its duties, become privy to or have access to sensitive and/or confidential information (verbal or written) including information that relates to, but is not limited to, police investigations and alerts, health care information, juvenile and criminal records, legal documents and other information not generally available to the public and deemed sensitive and/or confidential by law ("Sensitive Information").

Pursuant to its contract with the City, Contractor has a need to access the Network that is owned, operated and maintained by the City. However, the City is unwilling to provide or permit access to the Network unless Contractor agrees to maintain the integrity and confidentiality of Sensitive Information. In order to properly safeguard the integrity and confidentiality of the City's Sensitive Information, Contractor shall adhere to the following:

1. Contractor has agreed to adhere to this Policy as part of its contract with the City. Contractor acknowledges that it will not disclose any Sensitive Information owned by the City to unauthorized persons as a result of using the Network for any purpose.

2. All information contained in the Network including, but not limited to network configuration, firewall configuration, host/server configuration, username/password pairs, access codes, any and all data contained on computers owned, operated, or maintained by the City is Sensitive Information.

3. Security of Sensitive Information is essential to the integrity and operation of the Network. Contractor will not permit unauthorized access to the Network and will not disclose network IDs and/or passwords to any person other than City IT Administrators or other authorized City personnel.

4. Contractor shall access the Network and use Sensitive Information only to the extent to which it is authorized and has a need in order to fulfill its obligations under its contract with the City. Contractor shall not aid or permit any unauthorized person to have access to the Network.

5. Contractor shall not knowingly or intentionally enter any erroneous, false or fraudulent information into the Network.

6. Contractor's authorization for the use of Sensitive Information and access to the Network shall cease upon the termination of Contractor's need and authorization to have access to such information pursuant to its contract with the City and/or the termination of its contract with the City.

7. Contractor must not disclose, copy, sell, loan or in any way divulge Sensitive Information to any unauthorized person and shall not modify, destroy or otherwise take any action that will alter Sensitive Information to which Contractor does not have security privileges.

8. All Sensitive Information, the Network, and any information pertaining thereto are the exclusive property of the City. Contractor must not copy or otherwise reproduce any Sensitive Information except as authorized under its contract with the City, or by a City employee. All copies or reproductions of Sensitive Information are the exclusive property of the City and shall be returned immediately to the City upon termination of the Contractor's purpose for having access to the Sensitive Information pursuant to its contract with the City and/or the termination of its contract with the City.

9. Contractor understands and agrees that it is prohibited from copying, transmitting or distributing any City information in violation of any local, State, federal or international laws, regulations, treaties, or City policies. These laws include, without limitation, those relating to confidential records, electronic privacy and computer fraud, abuse and trespass laws, copyright, trademark, trade secret laws, obscenity laws, and U.S. and foreign government regulations relating to the exportation and/or importation of data.

10. Any contacts by Contractor with press or media representatives must be reported to the City Public Information Office and/or other appropriate City Offices.

11. Contractors who violate this Policy may be subject to termination of their contract with the City and/or legal action.