**CITY OF MADISON, WISCONSIN**

**Information Technology Network Connection Agreement**

1. **PURPOSE**

The purpose of this Network Connection Agreement (“Agreement”) is to ensure that a secure method of network connectivity is provided between the City of Madison (“City”) and [FULL LEGAL BUSINESS NAME OF CONTRACTOR], an external organization, entity, or individual that provides software support, maintenance, network services, and/or system development services to the City (“Contractor”), and to provide guidelines for the use of network and computing resources associated with Contractor’s Network Connection as defined below.

1. **DEFINITIONS**

“Affiliate” means another entity, including, but not limited to, another unit of local government, for which the City of Madison provides network services and access to the City Network.

“City Property” is defined in Section 7.A. and includes, but is not limited to, all data of the City of Madison and its Affiliates.

“Confidential Information” means protected health information subject to the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations, as amended from time to time (“HIPAA”), any records related to juveniles, information gathered by law enforcement in ongoing investigations, network security information, the collection of any of the following in connection with a person or business’s name: dates of birth, social security number, driver’s license or state identification number, financial or credit/debit card account numbers, payroll information, tax forms, trade secrets, security/access codes, PINs or passwords, or any other sensitive information/records that could be used for identity theft or other forms of fraud, and any other information where the City’s record custodian declares the private reputational interest outweighs the public interest in release.

“City Network” means the City of Madison’s collection of computers and other hardware and software interconnected by communication devices that allows for the sharing of resources and information by employees of the City of Madison and its Affiliates.

“Network Connection” means a connection between the City Network and the network of the Contractor. Under this Agreement, only the connectivity methods listed below shall be used to establish a Network Connection, unless another method is approved by the City as described below:

1. Virtual Private Network (VPN). If connecting via VPN, the Contractor must use a City-approved VPN client and authentication method as specified below. The City may discontinue the VPN option on notice to the Contractor, at which time another approved connection method will be required.
2. Remote Access Tool. The Contractor may connect using a specific remote access product that must be cleared for use in writing by the City in advance. If using the remote access tool method, the City must initiate and terminate all connections. Pre-approved remote access tools include WebEx and Go To Assist. If another tool is required, it must be approved by IT prior to its use.
3. Non-Persistent RDP Connection. The Contractor may use a non-persistent RDP connection via the City’s virtual desktop environment.
4. Other Connection Methods. The City’s connectivity options listed above are the standard methods of providing a connection to the City Network to the Contractor. Anything that deviates from these standard methods must be approved in writing by the City Chief Information Officer (“CIO”) or their designee.

Connection Requests and Approvals. All requests for Contractor Network Connections must be made via the City’s contact person in Section 5.

Authentication for Network Connections. All Network Connections must be authenticated using the City’s authentication database or other authentication methods approved by the City in writing.

Changes to Connection Method. All requests for any type of change to the Network Connection, or an approval request for another method, must be made in writing and submitted to IT@cityofmadison.com. A change between one of the approved methods above may require additional set-up and/or configuration.

If, at any time, the Contractor’s Network Connection does not meet the requirements of this Agreement, the City reserves the right to have the Contractor meet the City’s current connection requirements, as needed, at the Contractor’s expense, or terminate the Network Connection.

1. **ACCESS PROVIDED**

In general, access provided to the Contractor over Network Connection should be limited only to what is needed, and only to devices (hosts, routers, etc.) needed, in the sole opinion of the City. The City will not provide blanket access. The City’s default policy position is to deny all access and only allow a Network Connection to perform specific services needed and approved by the City. Access to resources such as SFTP, databases, etc. must be outlined in accompanying documentation and agreed to by the City.

1. **APPROPRIATE USE OF NETWORK CONNECTION**

The Contractor may only use the Network Connection in compliance with this Agreement and only to:

1. Perform services described in the contract or purchase order through which this Agreement is attached or incorporated (“Contract”); or
2. If not pursuant to any Contract, the Contractor shall only establish a Network Connection at the request of the City and only for the reasons that the Connection was requested by the City. The City will only request such a connection for its legitimate business purposes.
3. The Contractor shall not access, download, or make copies of City Property, which includes data, without the City’s written permission. Such permission shall only be given pursuant to the express terms of a written contract between the City and Contractor to which this Agreement is attached or incorporated.
4. In no case shall the Contractor use the City’s Network, including the City’s internet connection, for personal use or any use other than approved under Sections 3.A and B. above.
5. **NETWORK SECURITY**
6. Contractor’s Authorized Employees. The Contractor will only allow the employees listed in Attachment A and approved by the City in advance (“Authorized Employees”) to access the City Network through a Network Connection. The Contractor shall inform all Authorized Employees listed on Attachment A of the requirements of this Agreement. The Contractor shall be solely responsible for ensuring that Authorized Employees are not security risks, and, upon the City’s request, the Contractor will provide the City with any information reasonably necessary for the City to evaluate security issues relating to any Authorized Employees.
7. Changes to Authorized Employees. The Contractor will promptly (within not more than five (5) business days) notify the City whenever any Authorized Employee leaves the Contractor’s employ or no longer requires access to the Network Connection, and that person’s name shall be removed from Attachment A. The Contractor shall also notify the City within five (5) business days of any changes in the contact information for an Authorized Employee listed on Attachment A, such as name, address, phone, or email. It is the Contractor’s responsibility to provide accurate and complete contact information for its Authorized Employees. Notices required by this Section shall be made to the City’s contact person in Section 5 below.
8. Contractor’s Security Protocols. The Contractor will be solely responsible for the selection, implementation, and maintenance of security procedures and protocols that are sufficient to ensure that (i) the Contractor’s use of the Network Connection is secure and is used only for authorized purposes, and (ii) the City’s records, data, and City Property are protected against improper or unauthorized access, use, loss, alteration, or destruction.
9. Security Breach Notification. The Contractor shall comply with any breach or incident notification procedures required in the underlying Contract (if applicable), or those required by HIPAA or applicable privacy laws, if the underlying Contract involves protected health information or personally identifiable information. The following notification requirements are in addition to any such requirements.

For the purposes of a Network Connection, a security breach includes any incident that results in unauthorized access to the City Network, City Property as defined herein, or City or Contractor’s networks, applications, or devices, resulting in information being accessed without authorization, and also includes a security incident such as a malware infection, DOS or DDOS attack, a lost or unattended device, whether such breach or incident occurs along the path of the Network Connection, or within the Contractor’s corporate network or any of the Contractor’s connected devices. The Contractor shall notify the City immediately of any such breach or incident that occurs while the Contractor is actively connected to the City Network or any time during the term of any Contract or business relationship with the City that could require a Network Connection. The Contractor shall notify the City of any breach or incident immediately of any breach or incident immediately as follows:

* Calling the IT Help Desk at (608) 266-4193 (available 24/7).
* The phone notification shall be followed up with an immediate email notification to IT@cityofmadison.com.
1. **NOTIFICATIONS AND PERMISSIONS**

The Contractor shall use the contact information below to request a Network Connection, to request a change in Network Connection method, and to notify the City of changes to Authorized Employees listed in Attachment A. In the absence of a separate written Contract, this Section will be used by the City to notify the Contractor of any violation of this Agreement, and the City’s intended response to the violation, including, but not limited to, termination of the Contractor’s Network Connection.

Notices from either party to the other via first-class, postage pre-paid mail, email, or hand delivery shall be sent to the following:

|  |  |
| --- | --- |
| FOR THE CITY: | City of Madison Assistant Director, Department of Information Technology |
| 210 Martin Luther King, Jr. Blvd., Room 500 |
| Madison, WI 53703 |
| Email: IT@cityofmadison.com |
|  |
| *With a copy to:* | City of Madison Chief Information Officer, Department of Information Technology |
| 210 Martin Luther King, Jr. Blvd., Room 500 |
| Madison, WI 53703 |
|  |
| FOR THE CONTRACTOR: |       |
|       |
|       |
| Email:       |

1. **CITY PROPERTY**
2. City Property is defined as all materials relating to the business and affairs of the City and its affiliates, including, without limitation, all manuals, documents, reports, equipment, working materials, content, messages, data, datasets, data structures, spreadsheets, entries, information, text, music, sound, photos, videos, graphics, code, or other items or materials, prepared by the City, its Affiliates, or by the Contractor for the City, whether or not such materials are also considered Confidential Information as defined herein.
3. City Property is for the benefit of the City and its Affiliates and is and shall remain the property of the City (or its Affiliates) at all times. Nothing about this Network Connection Agreement grants or transfer the Contractor or any other party any ownership rights or license to City Property.
4. If the Contractor’s access to the Network Connection is pursuant to a Contract between the City and the Contractor, the parties intend on all provisions of such Contract, including any provision regarding data ownership, ownership of Contract product, license grants, and intellectual property to be read together with this Network Connection Agreement, and harmonize to the extent possible. In the event of a conflict between such Contract and this Agreement, the provision that more strictly protects City Property and preserves the City’s ownership rights in City Property shall apply.
5. This Agreement should not be interpreted to transfer or otherwise modify the ownership of the Contractor’s intellectual property, if any, contrary to the terms of the Contract or any related license agreement executed by the City and Contractor.
6. **TREATMENT OF CITY PROPERTY AND CITY’S CONFIDENTIAL INFORMATION**
7. The Contractor acknowledges that it may receive and have access to the City’s Confidential Information, as defined herein, when making a Network Connection.
8. If the Contractor’s connection to the City Network is pursuant to a Contract between the City and the Contractor, the parties intend all provisions of such Contract, including any confidentiality provision to be read together with this Agreement and harmonize to the extent possible. In the event of a conflict between such Contract and this agreement, the provision that more strictly protects the City’s Confidential Information, as defined herein, shall apply.
9. All right, title, and interest in and to City Property and the City’s Confidential Information shall remain the exclusive property of the City and the Confidential Information shall be maintained in confidence and held in trust by the Contractor for the benefit of the City. The Contractor shall not, directly or indirectly, use or exploit City Property or the City’s Confidential Information for any operational, commercial, or other purpose whatsoever, or in any manner detrimental to the City or its Affiliates, or disclose, disseminate, impart, or grant access to City Property or the City’s Confidential Information to any person for any purpose.
10. The Contractor shall not copy, reproduce in any form, or store in any retrieval system or database City Property or the City’s Confidential Information without the prior written consent of the City, except for such copies, reproductions, and storage as may be reasonably required internally by the Contractor for the purpose for which Contractor receives City Property or the City’s Confidential Information through the Network Connection.
11. The Contractor agrees that at no time shall the Contractor, its employees or agents, authorize a third-party to have access to the City Network.
12. Contractor Information. The City shall not have any responsibility for ensuring the protection of the Contractor’s information unless explicitly agreed in writing. The Contractor shall be entirely responsible for providing the appropriate security measures to ensure the protection of its private internal network and information.
13. **SIGNATURE**
14. Contract for Purchase of Services. If this Agreement is referenced and incorporated into a Contract for Purchase of Services or other contract between the Contractor and the City, then the Agreement applies to the Contractor by virtue of the Contractor’s signature on the underlying contract and no further signature is required for the Contractor to be bound to this Agreement.
15. Stand-Alone Document. If this Agreement is presented to the Contractor without an underlying contract, the Contractor makes the following acknowledgement: By signing below, I acknowledge that I have read and received a copy of this Network Connection Agreement and agree to be bound by the terms herein.
16. **COUNTERPARTS, ELECTRONIC SIGNATURE, AND DELIVERY**

This Agreement may be signed in counterparts, each of which shall be taken together as a whole to comprise a single document. Signatures on this Agreement may be exchanged between the parties by facsimile, electronic scanned copy (.pdf) or similar technology and shall be valid as original; and this Agreement may be converted into electronic format and signed or given effect with one or more electronic signature(s) if the electronic signature(s) meets all requirements of Wis. Stat. ch. 137 or other applicable Wisconsin or Federal law. Executed copies or counterparts of this Agreement may be delivered by facsimile or email and upon receipt will be deemed original and binding upon the parties hereto, whether or not a hard copy is also delivered. Copies of this Agreement, fully executed, shall be as valid as an original.

|  |
| --- |
| **CONTRACTOR** |
|  |
| Authorized Signature (Contractor only signs if required by paragraph 9.B.) |
|       |
| Name |
|       |
| Title |
|       |
| Date |

**ATTACHMENT A: AUTHORIZED EMPLOYEES**

|  |  |  |  |
| --- | --- | --- | --- |
| **Employee Name** | **Telephone Number** | **Address** | **Email Address** |
|       |       |       |       |
|       |       |       |       |
|       |       |       |       |