WRIGHT COUNTY
MINNESOTA

Information Technology Usage Agreement
Vendor/Contractor/Volunteer

All employees, volunteers and agents of vendors and contractors who will access Wright County information technology in the course of their work for Wright County ("vendor personnel") are required to read and sign this document before accessing any Wright County computer system. "Information technology" includes any Wright County owned, leased, or operated computer, network, Internet access, electronic mail and voice message systems, facsimile devices, or other electronic systems used by Wright County. Vendor personnel have no expectation of privacy in any Wright County electronic communications, use of Wright County property, or Internet access. Wright County reserves the right to review, audit, or monitor any information technology used by vendor personnel. All work shall be performed by the contractor submitting the proposal. Subcontractors will not be allowed unless approved in advance by an agent of the County. This agreement does not apply to non-County owned systems. **Non-supervised access to CJDN requires additional agreements.**

1. Vendor personnel have no expectation of privacy in any electronic communications, use of Wright County property, or Internet access. Wright County reserves the right to review, audit, or monitor any information technology used by vendor personnel.
2. All vendor personnel shall use only accounts authorized by Wright County's IT Staff when accessing Wright County systems.
3. Vendor personnel may access only those resources for which they are specifically authorized.
4. Vendor personnel are personally responsible for safeguarding their Wright County account and log-on information. Passwords shall adhere to the following.
   a. Passwords shall remain confidential.
   b. Passwords shall be changed every 60 days.
   c. Passwords shall be at least 8 characters long.
   d. Passwords shall contain characters from at least two of the following 3 classes: (i) number, (ii) special, non-alphanumeric character, (iii) English capital letter.
   e. Passwords may not contain your user name or any part of your full name.
   f. Passwords shall never be displayed, printed, or otherwise recorded in an unsecured manner.
5. Vendor personnel are not permitted to script their user IDs and passwords for log-on access.
6. Vendor personnel are not permitted to allow another person to log-on to any computer utilizing their, if provided, personal account, nor are they permitted to utilize someone else's account to log-on to a computer. Authorized system or service accounts may be used by multiple people.
7. Vendor personnel may not leave their workstation logged onto the network while away from their area. Vendor personnel may elect to lock the workstation rather than logging off when leaving for very short time periods.
8. Vendor personnel shall execute only applications that pertain to their specific contract work.
9. Vendor personnel shall promptly report log-on problems or any other computer errors to the Helpdesk (763-684-2300).
10. Vendor personnel shall promptly notify the Wright County IT Department if they have any reason to suspect a breach of security or potential breach of security.
11. Vendor personnel shall promptly report anything that they deem to be a security loophole or weakness in the computer network to the Wright County IT Department.
12. Vendor personnel shall not install or use any type of encryption device or software on any Wright County hardware, which has not been approved in writing by the Wright County IT Department.
13. Vendor personnel shall not attach any device to the Wright County network without written approval from the Wright County IT Department.
14. Vendor personnel may not remove any computer hardware from any Wright County building for any reason, without prior written approval from the Wright County IT Department.
15. Vendor personnel shall not delete, disable, or bypass any authorized encryption device, or anti-virus or other software program, installed on Wright County hardware.
16. Vendor personnel may not copy any data and/or software from any Wright County resource for personal use.
17. Wright County data and/or software shall not be removed from a Wright County Building or network without prior written approval from the County.

18. Vendor personnel are prohibited from intercepting or monitoring network traffic by any means, including the use of network sniffers, unless authorized in writing by the Wright County IT Department.
19. Vendor personnel may not utilize Wright County computer systems or networks for any of the following reasons:
    a. Game playing
    b. Internet surfing not required for their work activity
    c. Non-Wright County related, work activity; including ANY personal use
    d. Any illegal activity
    e. Unapproved downloading of files from the Internet. If files are needed for your work, contact Wright County IT personnel
    f. Access any non-Wright County E-mail (Vendors may access other e-mail via the Wright County Guest Wi-Fi Internet network)
    g. Interfering with County Business
    h. Vendor personnel may not use Wright County information technology to send or receive threatening, obscene, abusive, sexually explicit language or pictures.
20. Vendor personnel may not give out any Wright County computer information to anyone. Exception: other vendor personnel needing the information to complete tasks and who have signed this agreement. Information includes but is not limited to: IP addresses, security configurations, etc.
21. All data storage media shall be erased or destroyed prior to disposal process must meeting current Federal standards for data destruction or deliver media to Wright County IT for destruction.
22. All county data or software, not residing on County Equipment shall be erased or destroyed upon completion of work.
23. Vendor personnel may not remove or delete any computer software without the written approval of the Wright County IT Department.
24. Vendor personnel shall not attempt to obtain or distribute Wright County system or user passwords.
25. Vendor personnel shall not attempt to obtain or distribute door pass codes/passkeys to secured rooms at any Wright County facility for which they are not authorized.
26. All equipment issued to vendor personnel will be returned in good condition to Wright County upon termination of the Wright County/Vendor Personnel relationship.
27. Vendor personnel are prohibited from causing Wright County to break copyright laws.
28. Vendor personnel may not disclose of any private or confidential client information regardless of physical form or storage media (paper, computer, voice mail, microfiche, imaged). Vendor personnel will not attempt to access not public data for personal purposes. Attachment 2 “Responsibilities of Persons Who Have Access to Not Public Data has been read and its’ conditions will be complied with by all vendor personnel.
29. Any vendor owned equipment that is used to access any Wright County Systems via any remote access or direct access system or connection must have current, licensed, updated and operating software including virus protection and appropriate firewall software. Use of non-vendor owned or controlled (personal) equipment (PC) is not allowed, internet connections and routers / access points are not included in this requirement. (Ok to use an Internet connection from a hotel, for example.)
30. The county is not liable for any damages to the vendor computer equipment that may occur while installing or using software or hardware connected to any County systems.
31. Use by vendor personnel of any Wright County information technology will acknowledge acceptance of the above-referenced policies. Violation of the agreement may result in immediate suspension of the Vendor Personal’s account. Any vendor employee who violates any of these policies shall be subject to disciplinary action, including total removal from the Wright County project as well as being subject to Minnesota civil and criminal liability. Disciplinary action may include Wright County requesting the vendor consider demotion, suspension and termination.

RESPONSIBILITIES OF PERSONS WHO HAVE ACCESS TO NOT PUBLIC DATA (VENDORS)

As a vendor working with Wright County, you may have access to records containing information which is protected from unauthorized use. For example, you may have access to special work areas, computers or other files. This information is protected by law, policy, contracts, agreements, or licenses regarding the disclosure both at work and outside the office.

Unauthorized use of data includes making copies of data or computer software and related materials without the permission of the originator or data subject. Unauthorized disclosure of data means releasing information over the phone, in verbal conversations, and in written form. Unauthorized disclosure also includes using the information obtained in connection with your vendor work duties in any manner different from the scope of your specified duties.

Protection of this data from unauthorized use or disclosure depends on the cooperation of all staff and vendors. The information in this handout explains some of these restrictions on information within the County so that you will understand what information is protected and your responsibilities in regard to that information.

NOT PUBLIC DATA

The following describes the private and confidential types of information, the restrictions on the use of it, and some examples of each type of information. Attached to the handout is a form which describes your responsibilities and states the type of private/confidential data to be collected and the purpose for which the summary data is being prepared (if applicable). Your signature on the form provides verification that you have read and understand these responsibilities.

Not public data means any data which the law declares is not available to the public. It is a broad term which includes private, nonpublic, confidential, or protected nonpublic data, either singly or in any combination.

Frequntly, if the data you work with identifies a person it is private or confidential data. Use and access within the agency is restricted to those employees or vendors who need the information to do their jobs.

A. Private data is government data maintained on individuals who are identified or can be identified in the data. Only the following persons are permitted access to private data:
   1. the individual who is the subject of the data or a designated representative;
   2. anyone to who the individual gives signed consent to view the data;
   3. employees whose work assignments reasonably require access to the data;
   4. anyone the law says can view the data

   Examples of private data include most welfare system data about individual clients, medical data, child abuse data, pre-commitment screening investigations and pre-admission screening investigations, chemical dependency data about patients, and personnel data.

B. Confidential data is data that identifies individuals and cannot be disclosed to the public or even to the individual who is the subject of the data. The subject of the data CANNOT authorize anyone else to see or receive copies of the data by signing a consent for release of information.

   Examples of confidential data are adoption data and the names of individuals who report child or vulnerable adult abuse. Some medical data is confidential if the medical care provider deems that access to the data will be harmful to the patient. Most investigations of individuals are confidential, but investigations involving corporations, agencies or vendors are protected nonpublic.

PENALTIES FOR UNLAWFUL USE OF DATA

The Minnesota Government Data Practices Act, MN Statutes, Chapter 13, provides for disciplinary action for any government employee who knowingly violates the provisions of the Act. Any person, even those who are not employees, who willfully violate the provisions of the Act, may be charged with a misdemeanor.

Action for Damages A political subdivision, responsible authority, statewide system, or state agency which violates any provision of this chapter is liable to a person or representative of a decedent who suffers any damage as a result of the violation, and the person damaged or a representative in the case of private data on decedents or confidential data on decedents may bring an action against the political subdivision, responsible authority, statewide system or state agency to cover any damages sustained, plus costs and reasonable attorney fees. In the case of a willful violation, the political subdivision, statewide system or state agency shall, in addition, be liable to exemplary damages of not less than $1000, nor more than $15,000 for each violation. The state is deemed to have waived any immunity to a cause of action brought under this chapter.

REQUIRED INSURANCE INFORMATION

The Contractor shall purchase, provide and maintain at its own expense, insurance coverage as stated in this agreement. Proof of insurance shall be furnished to Wright County prior to the commencement of any work and shall be maintained throughout the life of this agreement and shall be evidenced by the carriers certificates, filed with the County. All insurance must meet current State of MN requirements.

- Minnesota Workers Comp Insurance/Employers Liability Insurance: Contractor shall procure and maintain a policy that at least meets Minnesota statutory minimum limits and is covered for work in Minnesota.
- Professional Liability Insurance:
- Certificate of Insurance: The insurance certificate shall specify Wright County as an additional insured and list the project name.

Description of Work to be done (if this work is being done for a contract, please reference which contract) :

Timeline:

Special Conditions (if Any):

Vendor Personnel's Signature **Date** **Vendor's Name, Printed**

Vendor personnel's name, printed **Vendor personnel's name, printed**

Wright County IT Manager **Date**

Non-CJDN vendor remote access only approved if signed above by an IT Manager (this approval is valid for term of this agreement or 1 year whichever is less).

For IT Office Use Only: Wright County User ID: