JEFFERSON COUNTY, WISCONSIN

REQUEST FOR PROPOSAL
AUDIT SERVICES
RFP 2019-2 FIN

CONTACT INFORMATION	
BUYER	Marc DeVries
E-MAIL	mdevries@jeffersoncountywi.gov
PHONE	920.674.7142
MAILING ADDRESS	311 S Center Ave, Room 109 Jefferson, WI 53549

SCHEDULE OF EVENTS	
The following dates are provided for your information and planning purposes. Although every effort will be made to follow this schedule, we reserve the right to modify the dates as necessary.	
RFP Released	June 21, 2019
Questions Due	4:00 PM CST, July 22, 2019
Proposals Due	3:00 PM CST, August 2, 2019
Finance Committee Approval	August 8, 2019
Award of Contract pending County Board approval	September 10, 2019
Commencement Date	October 1, 2019

TABLE OF CONTENTS

REQUEST FOR PROPOSAL

PREPARATION, SUBMISSION, PROCESS AND AWARD

1. Communication:

This RFP is issued on behalf of Jefferson County by the Finance Department. The buyer assigned to this RFP, along with contact information, is noted on Page 1. The buyer is the sole point during this process and no information provided by any personnel will be considered binding.

The County prohibits communication initiated by the respondent to any County official, employee or representative evaluating or considering the proposals, prior to the time an award has been made.

All respondents should use this written document, its attachments and any amendments as the sole basis for responding.

2. Access to County Building:

Controlled access screening is mandatory for all vendors seeking access to the Courthouse. Vendors who will be visiting are to enter and exit the facilities through the main Courthouse public entrance 311 S Center Avenue. Screening will take place in the lobby of the Courthouse. Allow sufficient time to get through the screening process if you are hand delivering your response.

3. Clarifications/Amendments:

If you discover any significant ambiguity, error, omission or other deficiency in the RFP, immediately notify the Buyer in writing. All other questions, clarifications or exceptions regarding the RFP document must be raised prior to the submission of the proposal. Please note the due dates and times noted on page 1 for questions regarding this request. In accordance with Section B on page 4 of this Request for Proposal, all questions must be submitted to the buyer in writing, via email, with the RFP description clearly identified as required.

If it becomes necessary to clarify or revise any part of this RFP, amendments will be posted to the Jefferson County website: http://www.jeffersoncountywi.gov/rfp, in accordance with the schedule on Page 1. It is the responsibility of prospective vendors to check the website for any amendments prior to the opening date. All amendments must be acknowledged on the RFP signature page in the area provided. **Failure to do so may result in your response being rejected.**

4. Contents of Proposal:

All attachments, additional pages, addenda or explanations supplied by the vendor with their proposal will be considered as part of the proposal response.

5. Nonconforming Terms and Conditions:

A response that includes contractual terms and conditions that do not conform to the contractual terms and conditions in the RFP document are **subject to rejection as nonresponsive.** Jefferson County reserves the right to permit the respondent to withdraw nonconforming terms and conditions from its response or negotiate changes to the contractual requirements prior to making a determination of responsiveness.

6. Amendment/Withdrawal of Proposals by Vendor:

After receipt by the Finance Department, vendor proposals may only be amended by submitting a later dated proposal that specifically states that it is amending an earlier proposal. No proposal may be amended after the opening date unless requested by the Finance Department.

Proposals may be withdrawn only in total, and only by a written request to the Finance Department prior to the time and date scheduled for opening of proposals.

completeness, and clarity of content. All parts, pages, figures, and tables should be numbered and clearly labeled. Instructions relative to each part of the response to this RFP are defined in the remainder of this section.

All proposals must be typed on standard 8 ½" x 11" paper (larger paper is permissible for charts, spreadsheets, etc.) separating each section. Respondent shall be required to mail one (1) original and five (5) copies of the proposal document in a sealed package, box or envelope to arrive no later than 3:00 P.M. CST on August 2, 2019.

Each hard copy should be double-sided and bound, with the exception of the original, which should be double-sided but not bound. The copies should be bound by staple, binder clip or in a three-ring binder. Spiral, wire or comb bound copies are also acceptable.

Responses should be identified in the lower left corner as follows:

PROPOSAL RESPONSE, **RFP # 2019-2 FIN Audit Services**

D. Pricing Document:

Pricing must be submitted on the form provided in Attachment D. Failure to do so may result in your proposal being rejected.

E. Mailing Address:

All hard copy submissions are to be mailed or delivered to:

Jefferson County
Finance Department, Room 109
311 S Center Avenue
Jefferson WI 53549

F. Hand Delivery:

If you are delivering your response in person, you must enter through the main courthouse entrance, 311 S Center Avenue, and deliver it to the Finance Department in Room 109 to be time stamped no later than 3:00 p.m. on the opening date.

G. Response Receipt/Opening:

Responses received after the due date and time will be rejected.

Proposals will be opened and the name of the respondents read; however, detail of each proposal, including proposed fees will not be announced at the time of opening. Such information shall be made public an award has been made and all negotiations are completed.

All proposals received in response to this request will become the property of the County and will not be returned to the respondents.

H. Interviews:

Interviews may be required of selected finalists at the respondent's expense. However, an award may be made without discussion with the respondents. Therefore, respondents are cautioned that proposals should be submitted initially on the most favorable terms, from both a technical and cost standpoint.

If an interview is required, the selected finalists will be notified of the date and time of the interview process. Vendors not selected will also be notified.

Proposers not selected will be notified that their proposal will no longer be considered unless the evaluation committee finds, after the completion of interviews, that additional proposers should be interviewed.

I. Financial Verification

Vendor verification prior to award: Vendor's financial solvency may be verified through financial background checks via Dun & Bradstreet or other means (i.e.; Wisconsin Circuit Court Access, UCC) prior to contract award. Jefferson County reserves the right to reject proposals based on information obtained through these background checks if it's deemed to be in the best interest of the County.

PROPOSAL FORMAT & SUBMISSION

A. Tentative Project Timeline

Please Note: These dates are for planning purposes. They represent the County's desired timeline for implementing this project. Any revision to the Due Date for submission of proposals will be made by addendum. All other dates may be adjusted without notice, as needs and circumstances dictate.

Issuance of RFP	June 2019
Proposal responses due from vendors	August 2, 2019 by 3 PM CST
Review proposal selections with Finance Committee	August 8, 2019
Award of contract pending County board approval	September 10, 2019
Send out Intent to Award/Thank You letters	September 12, 2019
Contract start date	October 1, 2019

B. RFP Questions

All questions related to this RFP must be in writing and received by the Jefferson Finance Department no later than 4:00 p.m. CST, July 22, 2019 via e-mail to marcd@jeffersoncountywi.gov . Clearly mark the e-mail: "Questions for RFP-Auditing Services". **Mailed, phone call and faxed questions will not be accepted.**

Answers to all written questions will be published in the form of an addendum and posted on the Jefferson County website at: (http://www.jeffersoncountywi.gov/rfp). It is the responsibility of all interested vendors to access the web site for this information. Calls for assistance with the web site can be made to (920) 674-7142.

C. Proposal Submission Requirements:

Proposal documents must be submitted in hard copy**.** Any deviation from these requirements may result in the proposal being considered non-responsive, and could eliminate the vendor from further consideration. The proposal shall be prepared with a straight forward, concise delineation of the vendor's capabilities to satisfy the requirements of this RFP including the following items outlined (1 – 5) below:

1. **Proposal Format (See Attachment B):**
   Include responses provided in this attachment in your proposal to be considered for this service.
2. **Proposal Rate Sheet (see Attachment D):**
   Provide all required elements of cost on this form.
3. **Proposal Reference Data Sheet (See Attachment E):**
   Provide attachment listing three to five references with your proposal.
4. **Proposal Designation of Confidential and Proprietary Information (See Attachment F):**
   If any part of your proposal includes proprietary and confidential information which qualifies as a trade secret, as provided in s. 19.36(5) Wis. Stats., or is otherwise material that can be kept confidential under the Wisconsin Open Records Law, please designate on the attachment and provide with your proposal. *Prices always become public information when bids/proposals are opened, and therefore cannot be kept confidential.*
5. **RFP Addendum Acknowledgement Receipt Schedule (See Attachment G):**
   If Addenda exist for this project, please sign and date the attachment and provide it with your proposal.

In order for the committee to adequately compare proposals and evaluate them uniformly and objectively, firms must complete the proposal in accordance with the guidance provided by the County in Attachment B.

Failure to provide a proposal in accordance with the stated format may result in your response being rejected.

Proposals should be prepared in a simple, cost effective format providing a straightforward, concise description of the vendor's capabilities to satisfy the requirements of the RFP. The use of elaborate materials and the inclusion of additional information that has no direct bearing on the project are not desired. Emphasis should be concentrated on accuracy,

J. Evaluation and Award:

Proposals will be evaluated in accordance with the criteria listed below. Award will be made to the responsive, responsible Contractor who complies with the requirements and scores the highest total on the evaluation criteria as it pertains to the overall needs of Jefferson County.

Quality and completeness of proposal	20%
Experience of firm in providing similar services and qualifications of staff assigned to provide service outlined in proposal	20%
Audit approach	20%
Cost	40%

K. Other Considerations:

Factors which include, but are not limited to, quantity involved, time of completion, purpose for which required, competency and financial capacity of vendor, ability to render satisfactory service and past performance will be considered in determining status as a responsible vendor. The County reserves the right to request additional information as may reasonably be required to make this determination and to further investigate the qualifications of the respondent as deemed appropriate.

All work shall conform to all applicable industry, federal, state and local laws, codes, ordinances, and standards.

The County prohibits communication initiated by the respondent to any County official, representative from another entity or employee evaluating or considering the proposals, prior to the time a decision has been made.

Interested vendors must inform the County Administrator, prior to proposal submission deadline, if they have any pre-existing business relationship(s) with the County related to this project that may conflict with a potential contract award.

Jefferson County reserves the right to accept or reject any or all proposals and to waive any informality in proposals. No vendor will be provided with financial and/or competitive vendor information on this proposal until after the award of contract has been made. To the extent possible, it is the intention of Jefferson County to withhold the contents of the proposal from public view until such times as competitive or bargaining reasons no longer require non-disclosure, in the opinion of Jefferson County. At that time, all proposals will be available for review in accordance with the Wisconsin Open Records Law. Jefferson County shall not be held liable for any claims arising from disclosure it determines is required under the Wisconsin Open Records Law.

Taxes: Jefferson County and its departments are exempt from payment of all federal tax and Wisconsin state and local taxes on its purchases except Wisconsin excise taxes.

This contract shall be subject to the laws of the State of Wisconsin. In connection with the performance of work under this contract, the contractor agrees not to discriminate against any employee or applicant for employment because of age, race, religion, color, handicap, sex, physical condition, developmental disability as defined in s.51.01(5), Stats., sexual orientation as defined in s.111.32(13m), WI Stats, or national origin.

Jefferson County is an Equal Opportunity Employer.

By responding to this proposal, prospective vendors acknowledge and accept the attachments, including the insurance requirements and standard contract template.

L. Reservations:

This RFP does not commit the County to pay any costs incurred in the preparation of a response to this request or to procure or contract for services or supplies. The Finance Department reserves the right to accept or reject any or all proposals received as a result of this request, request additional information, waive minor irregularities in the procedure, negotiate with any qualified source, or to cancel this RFP in part or in its entirety.

M. Non-Interest of County Employees and Officials:

No County official, employee or representative on the evaluation committee shall have any financial interest, either direct or indirect, in the proposal or contract or shall exercise any undue influence in the awarding of the contract.

N. Contract Documents:

The successful vendor will be required to execute the following contract document (s) as applicable:

Yes/No	Description of Contract
Yes	Jefferson County's Service Contract
Yes	WI DHS Business Associate Agreement
Yes	IT Acceptable Use Policy

These documents are included as Attachment J to this proposal. These documents are not to be executed at this time nor returned with your response; they will only be required of the successful vendor.

O. RFP Tabulations:

RFP tabulations are available to the public after contract execution, approximately 60-90 days from the date of the opening. RFP Tabulations can be found at our website http://www.jeffersoncountywi.gov/rfp. If you are unable to access the internet, you may contact 920-674-7101 for a hard copy. Copies are 15 cents per page plus postage costs if applicable.

Attachment A

(Potential vendors are expected to perform the following service in order to submit a proposal and to be awarded a contract.)

Defining Scope of Work
Jefferson County RFP for Auditing Services

1. BACKGROUND

Jefferson County is requesting proposals from qualified firms of certified public accountants to audit its financial statements for the fiscal years ending December 31, 2019, 2020, 2021 with two (2) optional subsequent fiscal years at the approval of the Finance Committee. These audits are to be performed in accordance with generally accepted auditing standards, the standards set forth for financial audits in the General Accounting Office's (GAO) *Government Auditing Standards*, the provisions of the federal Single Audit Act of 1984 (as amended in 1996) and 2 CFR 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* as well as the following additional requirements:

1. Wisconsin Single Audit Guidelines as published by the Wisconsin Department of Administration,
2. All other related applicable Wisconsin state statutes.

2. CONTRACT TERM

Initial term of contract will be for three (3) years with the option of two (2) additional one (1) year renewals, subject to the annual review and recommendation of the Administrator, Finance Department, and Finance Committee, the satisfactory negotiation of terms (including a price acceptable to both Jefferson County and the selected firm), the concurrence of the Jefferson County Board of Supervisors and the annual availability of an appropriation.

3. NATURE OF SERVICES REQUIRED

A. Scope of Work To Be Performed:

Jefferson County desires the auditor to express an opinion on the fair presentation of its basic financial statements in conformity with generally accepted accounting principles.

The auditors will be required to express an opinion on the financial statements based on an audit. The auditor is required to audit the financial statements of the governmental activities, the business-type activities, each major fund, and the aggregate remaining fund information of Jefferson County. The report shall be issued in accordance with Government Auditing Standards, to include internal control over financial reporting and tests of its compliance with certain provisions of laws, regulations, contracts and grant agreements and other matters.

The auditor is not required to audit the introductory section of the report or the statistical section of the report. The auditor is not required to audit the management's discussion and analysis, however should apply certain limited procedures regarding the methods of measurement and presentation of the required supplementary information.

The auditor shall also be responsible for performing certain limited procedures involving required supplementary information required by the Governmental Accounting Standards Board as mandated by generally accepted auditing standards.

The auditor shall be required to issue an independent auditor's report on compliance with requirements applicable to each major Federal and State program and on compliance, internal control over compliance, and the Schedules of Expenditures of Federal and State Awards in accordance with 2 CFR 200 and *Wisconsin Single Audit Guidelines* issued by the Wisconsin Department of Administration.

B. Auditing Standards To Be Followed:

To meet the requirements of this request for proposals, the audit shall be performed in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the provisions of the Single Audit Act of 1984 (as amended in 1996) and the provisions of 2 CFR 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards* and the *State Single Audit Guidelines* issued by the Wisconsin Department of Administration.

C. Reports to be issued:

Following the completion of the audit of the fiscal year's financial statements, the auditor shall issue:

1. A report on the fair presentation of the financial statements in conformity with generally accepted accounting principles, including an opinion on the fair presentation of the supplementary schedule of expenditures of federal and state awards in relation to the audited financial statements.

2. A report on compliance and internal control over financial reporting based on an audit of the financial statements.

3. A report on Federal and State Financial Awards which includes compliance and internal control over compliance applicable to each major program. Upon completion of the reports the auditor will complete the Data Collection Form and submit to the County.

In the required reports on compliance and internal controls, the auditor shall communicate any reportable conditions found during the audit. A reportable condition shall be defined as a significant deficiency in the design or operation of the internal control structure, which could adversely affect the organization's ability to record, process, summarize and report financial data consistent with the assertions of management in the financial statements.

Reportable conditions that are also material weaknesses shall be identified as such in the report. Non-reportable conditions discovered by the auditors shall be reported in a separate letter to management, which shall be referred to in the reports on compliance and internal controls.

The report on compliance and internal controls shall include all material instances of noncompliance. All nonmaterial instances of noncompliance shall be reported in a separate management letter, which shall be referred to in the report on compliance and internal controls.

Irregularities and illegal acts. Auditors shall be required to make an immediate, written report to Jefferson County's Finance Director or County Administrator of all irregularities and illegal acts or indications of illegal acts of which they become aware.

Reporting to the Finance Committee. Auditors shall assure themselves that Jefferson County's Finance Committee is informed of each of the following:

1. The auditor's responsibility under generally accepted auditing standards
2. Significant accounting policies
3. Management judgments and accounting estimates
4. Significant audit adjustments
5. Other information in documents containing audited financial statements
6. Disagreements with management
7. Management consultation with other accountants
8. Major issues discussed with management prior to retention
9. Difficulties encountered in performing the audit

D. Special Considerations:

1. Jefferson County will send its comprehensive annual financial report to the Government Finance Officers Association of the United States and Canada for review in their Certificate of Achievement for Excellence in Financial Reporting program. It is anticipated that the auditor will

be required to provide special assistance to Jefferson County to meet the requirements of that program.

2. Jefferson County currently anticipates it will prepare one or more official statements in connection with the sale of debt securities which will contain the general purpose financial statements and the auditor's report thereon. The auditor shall be required, if requested by the fiscal advisor and/or the underwriter, to issue a "consent and citation of expertise" as the auditor and any necessary "comfort letters." Fees related to these offerings will be negotiated separately from the audit services described herein at the time of issuance.

3. Jefferson County has determined that the United States Department of Health and Human Services will function as the cognizant agency in accordance with the provisions of the Single Audit Act of 1984 (as amended in 1996) and 2 CFR 200, *Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards*.

4. The Schedule of Expenditures of Federal and State Awards and related auditor's report, as well as the reports on compliance and internal controls are not to be included in the comprehensive annual financial report, but are to be issued separately.

5. A list of findings and other weaknesses from Jefferson County's most recent financial statement audit is available upon request.

6. It is anticipated that the auditor will be required to provide assistance to Jefferson County to comply with new GASB pronouncements.

E. Working Paper Retention and Access to Working Papers:

All working papers and reports must be retained, at the auditor's expense, for a minimum of three (3) years from final payment, unless the firm is notified in writing by Jefferson County of the need to extend the retention period. The auditor will be required to make working papers available, upon request, to the following parties or their designees:

1. Jefferson County
2. State of Wisconsin Department of Health and Human Services
3. U.S. General Accounting Office (GAO)
4. Parties designated by the federal or state governments or by Jefferson County as part of an audit quality review process
5. Auditors of entities of which Jefferson County is a sub recipient of grant funds

In addition, the firm shall respond to the reasonable inquiries of successor auditors and allow successor auditors to review working papers relating to matters of continuing accounting significance.

4. JEFFERSON COUNTY GOVERNMENT DESCRIPTION

A. Primary Contact:

After the contract is awarded, the auditor's principal contact with Jefferson County will be the Finance Director, or a designated representative, who will coordinate the assistance to be provided by Jefferson County to the auditor. Names of contacts and telephone numbers will be provided to the successful audit firm.

B. Background Information:

Jefferson County serves an area of 576 square miles with a population of 84,352 per 2019 estimated census. Jefferson County's fiscal year begins on January 1 and ends on December 31.

Jefferson County provides the following services to its citizens:
Public safety, health and human services, conservation and development, education and recreation, highways, support for the State's judicial system, and general administrative services.

Jefferson County employs over 500 full and part-time employees and is organized into 28 departments and agencies. The accounting and financial reporting functions of Jefferson County are a combination of both centralized and decentralized activities. Human Services, Health and Highway have their own accounting staff.

Jefferson County has offices located throughout the City of Jefferson. Travel between offices will be required during this engagement.

More detailed information on the government, finances and organizational chart can be found in the 2018 Comprehensive Annual Financial Report and the 2019 Adopted Budget on the County's intranet site at http://www.jeffersoncountywi.gov .

C. Fund Structure:

Jefferson County uses the following fund types and account groups in its financial reporting.

FUND TYPE	NUMBER OF FUNDS
General fund	1
Special revenue funds	2
Debt service funds	1
Capital projects funds	1
Permanent funds	0
Enterprise funds	1
Internal service funds	0
Private-purpose trust funds	0
Investment trust funds	0
Pension trust funds (& other employee benefits)	0
Agency funds	0
Component unit	1

D. Budgetary Basis of Accounting:

Jefferson County prepares its budgets on a basis consistent with generally accepted accounting principles. It is not the practice of the County to include the statutory budget of the proprietary funds in the basic financial statements.

E. Federal and State Awards:

Please refer to the single Audit Report for the year ended December 31, 2018 for a listing of state and federal major and non-major financial assistance programs. See Attachment J.

F. Pension Plans:

Jefferson County participates in the Wisconsin Retirement System, a cost-sharing multiple-employer public employee retirement system. This is a defined benefit retirement program.

G. Other Postemployment Benefits:

Jefferson County participates in two postemployment benefit plans, a single-employer health insurance program, and the Local Retiree Life Insurance Fund (LRLIF) sponsored by the Wisconsin Department of Employee Trust Funds (ETF).

H. Component Units:

Jefferson County is defined, for financial reporting purposes, in conformity with the Governmental Accounting Standards Board's *Codification of Governmental Accounting and Financial Reporting Standards*, Section 2100. Using these criteria, component units are included in Jefferson County's financial statements. Jefferson County has one component unit that originated in 2019.

I. Magnitude of Finance Operations:

The Finance Department is headed by a Director and consists of a total of 4.7 employees.

J. Computer Systems:

Jefferson County's accounting records are maintained through the use of an automated budgeting, human resources, and accounting package (Tyler Munis). The annual budget, including revenues, appropriations and expenditures are recorded in the accounting records upon adoption by the County Board of Supervisors.

The Management Information Systems Department (MIS) supports the County's computer network of approximately 500 personal computers along with a mainframe system and internal network. Included in the on-line systems are the following primary systems:

- Tyler Munis ERP software
  - Accounts Payable/Purchasing
  - General ledger
  - Cash receipting
  - Payroll/Human Resources
  - Budgeting
  - Capital Assets
- JD Edwards (legacy accounting system, read only access)
- County Tax System for Real Estate/Personal Property
- State of Wisconsin KIDS System
- Sheriff/Jail Information System (CIS)
- Land Records Information System (GIS)
- Highway Accounting System (CHEMS)
- Human Services (EDALS, WISACWIS and AODA)
- Executime Timecard System (Tyler)

K. Availability of Prior Audit Reports and Working Papers:

Interested proposers who wish to review prior year's CAFR can access the report on-line at http://www.jeffersoncountywi.gov/Reports/Misc.%20Annual%20Reports/CAFR.pdf. The website address for Jefferson County is www.jeffersoncountywi.gov .

L. Schedule for the fiscal year audit:

Each of the following should be completed by the auditor no later than the dates indicated. Due to various deadlines, no extensions will be granted to the following timeline.

1. Interim Work: The auditor shall complete interim work prior to or during December.

2. Detailed Audit Plan: The auditor shall provide Jefferson County by December 1 both a detailed audit plan and a list of all schedules to be prepared by Jefferson County.

3. Fieldwork: The auditor shall complete all fieldwork by May 8.

4. Draft Reports: The auditor shall provide all draft financial statement recommendations, revisions and suggestions for improvement along with any recommendations to management to be available for review by the Finance Department by June 5.

5. Entrance Conferences, Progress Reporting and Exit Conferences (A similar time schedule will be developed for audits of future fiscal years if Jefferson County exercises its option for additional audits).

At a minimum, the following conferences should be held by the dates indicated on the schedule:

a. Entrance conference with all key finance department personnel and staff of key offices or programs prior to commencement of preliminary field work in a department. The purpose of this meeting will be to discuss prior audit problems and the interim work to be performed by the auditor and schedules/information to be provided by the Finance Department. This meeting will also be used to establish overall liaison for the audit and to make arrangements for work space and other needs of the auditor.

b. Progress conference with Department Heads upon completion of field work in a Department. The purpose of this meeting will be to summarize the results of the preliminary review and to identify the key internal controls or other matters to be tested.

c. Progress conference with key Finance Department personnel upon completion of preliminary field work. The purpose of this meeting will be to summarize the results of the preliminary review and to discuss schedules/information to be provided by the Finance Dept. for year-end work. Any anticipated findings should also be discussed.

d. Entrance conference with key Finance Department personnel to commence year-end audit work prior to commencement of year-end audit work.

e. Exit conference with department heads of key offices or programs immediately upon completion of field work in a department other than Finance. The purpose of this meeting will be to summarize the results of the field work and to review significant findings.

f. Exit Conference with key Finance Department personnel upon completion of field work (historically, the last day of fieldwork). The purpose of this meeting will be to summarize the results of the field work and to review significant findings.

M. Date Final Report is due:

Annually, Jefferson County Finance personnel shall prepare draft financial statements, notes and all required supplementary schedules and statistical data by April 30. The auditor shall provide all recommendations, revisions and suggestions for improvement to the Finance Director on or about May 30. A revised report, including draft auditor's reports shall be delivered to the Finance Director within one week of providing the draft report.

The Finance Department will complete their review of the draft report as expeditiously as possible. During that period, the auditor should be available for any meetings that may be necessary to discuss the audit reports. Once all issues for discussion are resolved, the final signed report shall be delivered to the Finance Director. It is anticipated that this process will be completed and available for final printing by Jefferson County no later than **June 15**.

The reconciliation of Form A with the Financial Statements shall be completed by the auditing firm no later than June 30.

The Federal Awards and State Financial Assistance Report and Management Communications shall be finalized and delivered to the Finance Director no later than **July 31.**

The final report, Federal Awards and State Financial Assistance Report and Management Communications should be emailed as a PDF file to the Finance Director.

5. ASSISTANCE TO BE PROVIDED TO THE AUDITOR AND REPORT PREPARATION

A. Finance Department and Other Assistance: The finance department staff and responsible management personnel will be available during the audit to assist the firm by providing information, documentation and explanations. The preparation of confirmations will be the responsibility of Jefferson County staff.

B. Accounting System (Munis) Assistance: The auditor will be provided a computer while onsite for onsite use and read-only access to Jefferson County's Munis software.

The use of Jefferson County's computer hardware and software will be limited to inquiry functions only for general ledger accounts and related receipts, disbursements and payroll journals.

C. Statements and schedules to be prepared by the staff of Jefferson County: The staff of Jefferson County will prepare numerous internal schedules with supporting documentation for each balance sheet account in each fund prior to the arrival of the auditors. In addition, special schedules for the auditors are prepared upon their request.

D. Jefferson County will provide the auditor with reasonable work space, desks and chairs. The auditor will also be provided with access to telephone lines and internet access.

E. The County currently prepares and prints the CAFR. The auditor prepares and prints the audit opinion on the financial statements, Federal Awards and State Financial Assistance Report, Report on Form A, Governance Communications, and Management Letter. (35 copies along with PDF files of all reports, except for the audit opinion on the financial statements, which is PDF only).

Attachment B

(Provide responses in the format below when submitting proposal to be considered)

Proposal Format

Jefferson County RFP for Auditing Services

The following details need to be provided in all submitted proposals to be considered for this service:

1. TITLE PAGE

Title page showing the request for proposals subject; the firm's name, address, phone number, fax number, website URL for your firm and any other firm or firms that you would team with, together with the name, address, phone, fax and e-mail for the person who should be contacted in regard to this RFP. If you propose to team with another firm, please provide the same information requested in this Statement for that firm.

2. TRANSMITTAL LETTER

A signed letter of transmittal briefly stating the proposer's understanding of the work to be done, the commitment to perform the work within the time period, a statement why the firm believes itself to be best qualified to perform the engagement and a statement that the proposal is a firm and irrevocable offer for 90 days for the audits for calendar years 2019, 2020, and 2021 and optional years 2022 and 2023.

3. FIRM QUALIFICATIONS AND EXPERIENCE

A firm resume describing the firm's experience with auditing Wisconsin governments. The proposer should state the size of the firm, the size of the firm's governmental audit staff, the location of the office from which the work on this engagement is to be performed and the number and nature of the professional staff to be employed in this engagement on a full-time basis and the number and nature of the staff to be so employed on a part-time basis.

If the proposer is a joint venture or consortium, the qualifications of each firm comprising the joint venture or consortium should be separately identified and the firm that is to serve as the principal auditor should be noted, if applicable.

The firm is also required to submit a copy of the report on its most recent external quality control review, with a statement whether that quality control review included a review of specific government engagements.

4. PARTNER, SUPERVISORY AND STAFF QUALIFICATIONS AND EXPERIENCE

Identify the principal supervisory and management staff, including engagement partners, managers, other supervisors and specialists, who would be assigned to the engagement. Indicate whether each such person is registered or licensed to practice as a certified public accountant in Wisconsin. Provide information on the government auditing experience of each person, including information on relevant continuing professional education and membership in professional organizations relevant to the performance of this audit.

Provide as much information as possible regarding the number, qualifications, experience and training, including relevant continuing professional education, of the specific staff to be assigned to this engagement. Indicate how the quality of staff over the term of the agreement will be assured.

The proposer should identify the extent to which staff to be assigned to the audit reflect Jefferson County's commitment to Affirmative Action.

Engagement partners, managers, other supervisory staff and specialists may be changed if those personnel leave the firm, are promoted or are assigned to another office. These personnel may also be changed for other reasons with the express prior written permission of Jefferson County. However, in either case, Jefferson County retains the right to approve or reject replacements.

Consultants and firm specialists mentioned in response to this request for proposal can only be changed with the express prior written permission of Jefferson County, which retains the right to approve or reject replacements.

Other audit personnel may be changed at the discretion of the proposer provided that replacements have substantially the same or better qualifications or experience.

5. INDEPENDENCE

The firm should provide an affirmative statement that is independent of Jefferson County as defined by generally accepted auditing standards/the U.S. General Accounting Office's *Government Auditing Standards*.

The firm also should provide an affirmative statement that it is independent of all of the component units of Jefferson County as defined by those same standards.

The firm should also list and describe the firm's professional relationships involving Jefferson County or any of its agencies, component units or primary government for the past five (5) years, together with a statement explaining why such relationships do not constitute a conflict of interest relative to performing the proposed audit.

6. LICENSE TO PRACTICE IN WISCONSIN

An affirmative statement should be included that the firm and all assigned key professional staff are properly licensed to practice in Wisconsin.

7. PRIOR ENGAGEMENTS WITH JEFFERSON COUNTY

List separately all engagements within the last five years, ranked on the basis of total staff hours, for Jefferson County by type of engagement (i.e., audit, management advisory services, other). Indicate the scope of work, date, engagement partners, total hours, the location of the firm's office from which the engagement was performed, and the name and telephone number of the principal client contact.

8. SIMILAR ENGAGEMENTS WITH OTHER GOVERNMENT ENTITIES

For the firm's office that will be assigned responsibility for the audit, list the most significant engagements (maximum - 5) performed in the last five years that are similar to the engagement described in this request for proposal. These engagements should be ranked on the basis of total staff hours. Indicate the scope of work, date, engagement partners, total hours, and the name and telephone number of the principal client contact.

9. SPECIFIC AUDIT APPROACH

The proposal should set forth a work plan, including an explanation of the audit methodology to be followed, to perform the services required in Attachment A of this request for proposal. In developing the work plan, reference should be made to such sources of information as Jefferson County's budget and related materials, organizational charts, manuals and programs, and financial and other management information systems. Proposers will be required to provide the following information on their audit approach:

a. Proposed segmentation of the engagement
b. Level of staff and number of hours to be assigned to each proposed segment of the engagement
c. Sample size and the extent to which statistical sampling is to be used in the engagement
d. Extent of use of EDP software in the engagement
e. Type and extent of analytical procedures to be used in the engagement
f. Approach to be taken to gain and document an understanding of Jefferson County's internal control structure
g. Approach to be taken in determining laws and regulations that will be subject to audit test work
h. Approach to be taken in drawing audit samples for purposes of tests of compliance
i. Approach to be taken in determining departmental visits

10. IDENTIFICATION OF ANTICIPATED POTENTIAL AUDIT PROBLEMS

The proposal should identify and describe any anticipated potential audit problems, the firm's approach to resolving these problems and any special assistance that will be requested from Jefferson County.

11. REPORT FORMAT

The proposal should include sample formats for required reports.

Attachment C

(This attachment is provided for your information only. There is no need to sign or mail it back.)

Proposal Scoring

Jefferson County RFP for Auditing Services

Responses to this RFP will be evaluated according to the following by a scoring team.

1. PROPOSAL EVALUATION PROCESS

The following steps will be observed in the evaluation of vendor proposals:

- **a.** Jefferson County will establish a proposal scoring team;
- **b.** The proposal scoring team will review all proposals received and score the proposals in accordance with the predefined scoring methodology;
- **c.** Composite scores will be developed summarizing the individual scoring efforts of each proposal scoring team member;
- **d.** Vendors will be ranked by composite score
- **e.** In order for proposals to be evaluated the following items are mandatory:
  - The audit firm is independent and licensed to practice in Wisconsin.
  - The firm has no conflict of interest with regard to any other work performed by the firm for Jefferson County.
  - The firm adheres to the instructions in this request for proposal on preparing and submitting the proposal.
  - The firm submits a copy of its last external quality control review report and management letter stating the firm has a record of quality audit work.
- **f.** Any proposal whose price is over-budget may not be scored or considered.

2. PROPOSAL SCORING METHODOLOGY

The following is a summary of the proposal evaluation factors and the point value assigned to each. These factors will be used in the evaluation of the individual vendor proposals. Points will be awarded on the basis of the following factors:

Specifications	Points
1. Quality and completeness of proposal	20
2. Qualifications of staff assigned to provide service	20
3. Audit approach	20
4. Cost	40
Total	100

3. EVALUATION FACTORS

The evaluation factors to be used in proposal scoring are described below:

- **a.** Quality and completeness of proposal: Proposals will be evaluated on how well the proposal is laid out in accordance with the RFP Requirements.
- **b.** Qualifications of staff assigned to provide service: The firm's past experience and performance on comparable government engagements, the quality of the firm's professional personnel to be assigned to the engagement and the quality of the firm's management support personnel to be available for technical consultation, experience with Wisconsin Counties, and experience with Single Audit.
- **c.** Audit Approach: Proposals will be evaluated on submitted Audit Approach including of proposed staffing plan for various segments of the engagement, adequacy of sampling techniques and adequacy of analytical procedures.
- **d.** Cost: Scoring is based on a formula with the lowest price submitted that is divided by the price of each prospective vendor times the established point value times the weight factor percentage.

Attachment D

(Use of this form is required when submitting proposal)

Proposal Rate Sheet

Jefferson County RFP for Auditing Services

Vendor Information:

Company Name: _____

Contact Person: _____

Address: _____

City, State, ZIP: _____

Phone: _____ Email: _____

Total all-inclusive price for 2019: _____
Total all-inclusive price for 2020: _____
Total all-inclusive price for 2021: _____
Total all-inclusive price for optional year 2021: _____
Total all-inclusive price for optional year 2022: _____

Breakdown for the audit of the 2019 financial statements

Personnel	Hours	Standard Hourly Rate	Quoted Hourly Rate	Quoted Total
Partners				
Managers				
Supervisory staff				
Other (specify):				
Subtotal				
Federal Awards and State				
Financial Assistance Report				
Out of pocket expenses				
Meals/lodging				
Transportation				
Other (specify):				
Total all-inclusive price for 2019 audit				

Rates should not be presented as a general percentage of the standard hourly rate or as a gross deduction from the total all-inclusive maximum price.

Notes:

The total all-inclusive maximum price to be proposed is to contain all direct and indirect costs including all out-of-pocket expenses. Jefferson County will not be responsible for expenses incurred in preparing and submitting the technical proposal or the sealed dollar cost proposal. Such costs should not be included in the proposal. Any applicable costs may include the following:

1. Rates by Partner, Specialist, Supervisory and Staff level times hours anticipated for each

2. The cost of special services should be disclosed as separate components of the total all-inclusive maximum price.

3. Any applicable out-of-pocket expenses Included in the total all-inclusive maximum price and reimbursement rates.

4. Any applicable rates for additional professional services.

5. If it should become necessary for Jefferson County to request the auditor to render any additional services to either supplement the services requested in this RFP or to perform additional work as a result of the specific recommendations included in any report issued on this engagement, then such additional work shall be performed only if set forth in an addendum to the contract between Jefferson County and the firm. Any such additional work agreed to between Jefferson County and the firm shall be performed at the same rates set forth in the schedule of fees and expenses included in the sealed dollar cost proposal.

6. Disclose any applicable fees associated with consultation or advice provided during the year on the proper accounting treatment of unusual events.

7. Disclose fees in connection with the sale of debt securities and an approximation of what the charge would be.

8. Disclose any applicable fees associated with telephone calls made during the year regarding financial reporting matters relating to the audit.

9. Disclose any applicable fees associated with telephone calls made during the year regarding

Attachment E

(Use of this form is required when submitting proposal)

Proposal Reference Data Sheet

Jefferson County RFP for Auditing Services

Provide a list of at least three and not greater than five clients that you are currently providing auditing services of similar scope.

You must verify that contact person listed is accurate and still employed with the company.

Agency: _____
Address: _____
Telephone: _____
Contact person: _____
Email address: _____

Agency: _____
Address: _____
Telephone: _____
Contact person: _____
Email address: _____

Agency: _____
Address: _____
Telephone: _____
Contact person: _____
Email address: _____

Agency: _____
Address: _____
Telephone: _____
Contact person: _____
Email address: _____

Agency: _____
Address: _____
Telephone: _____
Contact person: _____
Email address: _____

Attachment F

(Use of this form is required when submitting proposal)

Proposal Designation of Confidential and Proprietary Information

Jefferson County RFP for Auditing Services

The attached material submitted in response to the RFP for auditing services includes proprietary and confidential information which qualifies as a trade secret, as provided in s. 19.36(5) Wis. Stats., or is otherwise material that can be kept confidential under the Wisconsin Open Records Law. As such, we ask that certain pages, as indicated below, of this bid/proposal response be treated as confidential material and not be released without our written approval.

Prices always become public information when bids/proposals are opened, and therefore cannot be kept confidential.

Blanket labeling of confidential/proprietary information in headers/footers of documents will not be considered as confidential/proprietary.

Information cannot be kept confidential unless it is a trade secret. Trade secret is defined in s. 134.90(1) (c), Wis Stats. as follows: "Trade secret" means information, including formula, pattern, compilation, program, device, method, technique or process to which all of the following apply:

1. The information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.
2. The information is the subject of efforts to maintain its secrecy that are reasonable under the circumstances.

We request the following pages not be released

Section	Page #	Topic

IN THE EVENT THE DESIGNATION OF CONFIDENTIALITY OF THIS INFORMATION IS CHALLENGED, THE UNDERSIGNED HEREBY AGREES TO **PROVIED LEGAL COUNSEL OR OTHER NECESSARY ASSISTANCE TO DEFEND THE DESIGNATION OF CONFIDENTIALITY AND AGREES TO HOLD JEFFERSON COUNTY HARMLESS FOR ANY COSTS OR DAMAGES ARISING** OUT OF THE COUNTY'S AGREEING TO WITHOLD THE MATERIALS.

Failure to include this form in the bid/proposal response may mean that all information provided as part of the bid/proposal response will be open to examination and copying. The County considers other markings of confidential/proprietary in the bid/proposal document to be insufficient. The undersigned agrees to hold the County harmless for any damages arising out of the release of any materials unless they are specifically identified above.

Company Name :_____

Authorized Representative:_____
Signature

Authorized Representative:_____
Type or Print

Date:_____

Attachment G

(If Addendums exist for this project, please sign and date and send with your proposal)

RFP Addendum Acknowledgement Receipt Schedule

Jefferson County RFP for Auditing Services

The undersigned acknowledges receipt of the following addendum:

Addendum #1_____ Initials _____

Addendum #2_____ Initials _____

Addendum #3_____ Initials _____

Addendum #4_____ Initials _____

The undersigned agrees with the following statement:
I have examined and carefully prepared the RFB/RFP/RFQ from the plans and specifications and have checked the same in detail before submitting the RFB/RFP/RFQ to Jefferson County.

Name_____
Signature

Date_____

If this RFB/RFP/RFQ is assigned a project number all vendors are responsible to check for addendums, posted on our web site at http://www.jeffersoncountywi.gov/rfp for this project prior to the due date. No notification will be sent when addendums are posted unless there is an addendum within three business days of RFB/RFP/RFQ due date.

Vendors that do not have Internet access are responsible for contacting the Finance Department at 920-674-7142 to ensure receipt of addendums issued.

RFBs/RFPs/RFQs that do not acknowledge addendums may be rejected.

All RFBs/RFPs/RFQs submitted will be sealed. Envelopes are to be clearly marked with required information. Sealed RFBs/RFPs/RFQs that are opened by mistake due to inadequate markings on the outside may be rejected and returned to the vendor.

Attachment H

(This attachment is provided for your information only. There is no need to sign or mail it back.)

Proposal Appeals Process

Jefferson County RFP for Auditing Services

To: Vendors
RE: Jefferson County Appeals Process

An appeal refers to a written request from a vendor for reconsideration of vendor selection on a RFB, RFQ or RFP.

Appeals may be submitted for the following purchases:

1. The item is a public work project bid under Section 55.52 (29) and 66.29 of the Wisconsin Statutes, or
2. The item price is $5,000 or more or the total order is $10,000 or more, and
3. Vendor selection was based on factual errors, or
4. The lowest price vendor was not selected, or
5. Failure by the County or its agents to adhere to the County's policies and procedures or other legal requirements.

Appeals shall be submitted in writing and should specify the factual error or policy, procedure or other legal requirement which has been violated. Vendor appeals are to be submitted to the County Administrator within 72 hours of receipt of rejection letter. Appeals not containing the necessary information or not filed on a timely basis shall be rejected by the County Administrator.

Submit to: Jefferson County Administration
311 S. Center Ave. Room 111
Jefferson, WI. 53549

Attachment I

(Potential vendors are required to meet the following insurance requirements in order to be awarded a contract. There is no need to sign or mail it back.)

Contract Insurance Requirements

Jefferson County RFP for Auditing Services

Hold Harmless

Vendor hereby agrees to release, indemnify, defend and hold harmless Jefferson County, their officials, officers, employees and agents from and against all judgments, damages, penalties, losses, costs, claims, expenses, suits, demands, debts, actions and/or causes of action of any type or nature whatsoever, including actual and reasonable attorney fees, which may be sustained or to which they may be exposed, directly or indirectly, by reason of personal injury, death, property damage, or other liability, alleged or proven, resulting from or arising out of the performance under this agreement by vendor, its officers, officials, employees, agent or assigns. Jefferson County does not waive, and specifically reserves, it's right to assert any and all affirmative defenses and limitations of liability as specifically set forth in Wisconsin Statutes, Chapter 893 and related statutes.

Insurance Requirements

Vendor, Contractor, Tenant, Provider, Organization or other (will be referred as Outside Contractor) shall provide and maintain at its own expense during the term of their agreement, the following insurance policies covering its operations hereunder are minimum requirements. Such insurance shall be provided on a primary basis by insurer(s) financially solvent and authorized to conduct business in the State of Wisconsin.

The Outside Contractor shall not commence work under this contract until all insurance required under this paragraph is obtained and such insurance has been approved by a County representative, nor shall any Outside Contractor allow subcontractors to commence work on their subcontract until all similar insurance requirements have been obtained and approved by a County representative. Notwithstanding any provisions of this section, and for purposes of this agreement, contractor acknowledges that its potential liability is not limited to the amounts of insurance coverage it maintains or to the limits required herein.

(1) Worker's Compensation Insurance and Employers Liability.
State Statutory workers' compensation Limits
Employer Liability, $500,000 each accident.

(2) Comprehensive General Liability (Occurrence Form).

- Products and Completed Operations
- Personal Injury and Advertising Liability
- Independent Contractors/Protective

Limits of Insurance — $1,000,000 per occurrence
$1,000,000 aggregate

(3) Business Automobile Liability. Business Automobile Liability covering all owned, hired, and non-owned vehicles.
Limits of Insurance — $1,000,000 per occurrence for bodily injury and property damage.

(4) Excess/Umbrella Liability.
Limit of Insurance — $1,000,000 per occurrence

Additional Insured
The Outside Contractor agrees that all liability coverage policies other than professional liability shall name Jefferson County as additional insured's with respect to: liability arising out of activities performed by or on behalf of the vendor/contractor: products and completed operations of vendor/contractor; premises owned, occupied or used by vendor; or automobiles owned, leased, hired or borrowed by vendor. The coverage shall contain no special limitations on the scope of protection to the County.

Adjustments to Insurance Coverage
The limits of liability as set forth herein shall be periodically reviewed and adjustments made so as to provide insurance coverage in keeping with increases in the Consumer Price Index and what is deemed to be prudent and reasonable by the County or its representatives. In the event that the County determines that the limits need to be adjusted at some time after the initial term of the contract, the County shall give notice to the contractor in writing of the new limits and the Contractor shall make such adjustments to its insurance coverage within 60 day of such notice.

Subcontractor
Subcontractors of the Outside Contractor shall also be in compliance with these requirements, including but not limited to, the submittal of a Certificate of Insurance that meet the same requirement outlined for the Outside Contractor.

Waiver of Subrogation
Insurers shall waive all subrogation rights against Jefferson County on all policies required under this requirement.

Cancellation Notice
Jefferson County will be given 30 days' notice in advance of cancellation, non-renewal, or material change in coverage.

Proof of Insurance
A valid Certificate of Insurance shall be issued to "Jefferson County" prior to commencement of work and meeting the requirements listed to avoid any interruption of normal business services and transactions. Certificates must bear the signature of the insurer's authorized representative.

The insurance certificate must be issued by companies licensed to do business in the State of Wisconsin or signed by an agent by the State of Wisconsin.

The certificates of insurance shall include a provision prohibiting cancellation of said policies except upon 30 days prior written notice to the County.

The certificates of insurance shall include reference to the **contract name or RFP number** in the description section of the certificate and listing **Jefferson County** as the additional insured.

The certificate of insurance will be delivered to Jefferson County prior to the execution of the contract.

Jefferson County
Finance Department
311 S Center Ave-Room 109
Jefferson, WI 53549

Special considerations will be given if the required amounts cannot be met. This will only take place after an insurance waiver form is completed.

**** Jefferson County shall be named as an additional insured with respects to liability coverage's other than professional liability and will be given 30 days' notice in advance of cancellation, non-renewal, or material change in coverage. A certificate of insurance evidencing such coverage's shall be placed on file with the County prior to commencement of work under this contract. ****

Attachment J

(This document is provided as a template to potential vendors as a requirement that this document is to be used to contract with the awarded vendor. There is no need to sign or mail it back at this time.)

JEFFERSON COUNTY
PROFESSIONAL SERVICES STANDARD CONTRACT TEMPLATE

Purchase/Service Description: Auditing Services

Time of Performance: 2019 thru 2021 with the option of two (2) additional one (1) year renewals

Total Amount of Contract: Not to exceed $_____

Performance, schedules and invoices will be approved by: Jefferson County Finance Director, 320 S Main Street, Room 109, Jefferson, WI 53549

This Jefferson County Professional Services Standard Contract ("Contract") is made and entered into on this _____ day of _____, 20__ by and between _____ (the "CONTRACTOR"), and Jefferson County, a body corporate organized under the Laws of Wisconsin (the "COUNTY") (Collectively referred to as the "parties" or in the singular as the "party").

WITNESSETH:

WHEREAS, the COUNTY, a governmental entity organized and existing as a body corporate pursuant to Wis. Stat. § 59.01, is in the business of providing certain governmental services to the COUNTY and its citizens;

WHEREAS, the CONTRACTOR, is in the business of providing said services and has made express and implied representations to the COUNTY of being capable, experienced and qualified to undertake and personally perform those services as are required in fulfilling all obligations under the terms and conditions of this Contract; and

WHEREAS, relying upon the CONTRACTOR'S above-referenced express and implied representations, the COUNTY now desires to engage and the CONTRACTOR now desires to be engaged as an independent contractor and not as an employee of the COUNTY to perform said services, all in accordance with the terms and conditions of this Contract. Work shall commence in accordance with the terms and conditions of this Contract after the CONTRACTOR has executed the Contract, and either: (a) has been notified in writing to commence the Performance of Services; or (b) has received from the COUNTY an original of the Contract that is complete and fully executed.

NOW THEREFORE, in consideration of the mutual promises contained herein and other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the COUNTY and the CONTRACTOR agree as follows:

1. **REQUIREMENTS:**
   The CONTRACTOR hereby agrees to be retained by the COUNTY and the COUNTY hereby agrees to retain the CONTRACTOR to perform the services in accordance with the terms and conditions of this Contract, which includes, but is not limited to:

   A. that the CONTRACTOR is required to do, perform, and carry out in a satisfactory, timely, and proper manner the services delineated in this Contract;

   B. that the CONTRACTOR is required to comply with requirements listed with respect to reporting on progress of the services, additional approvals required, and other matters relating to the performance of the services under this Contract; and

C. that the CONTRACTOR is required to comply with time schedules and payment terms.

The CONTRACTOR and its subcontractors, to the same extent as the CONTRACTOR, agree to fulfill all obligations described in the COUNTY'S _____ (hereinafter referred to as the "Project"), as well as the addenda attached thereto, copies of both which are attached hereto and incorporated herein by reference**.**

The total amount of the Contract includes all services, deliverables, and reimbursable expenses. Additional reimbursable fees will not be accepted.

2. SPECIFIC CONDITIONS OF PAYMENT: Payment to be due and owed following completion and acceptance of the Project by the COUNTY. Payment will be made within thirty (30) days after receipt of a properly documented invoice, the manner of which is more fully set forth below under "Payment Schedule", but only if completion is deemed satisfactory by the COUNTY.

Payment Schedule

Net 30 days from receipt of a properly completed invoice to be mailed or emailed directly to:
Mail Address: Jefferson County Finance Director, 311 S Center Ave., Room 109, Jefferson, WI 53549
Email Address: marcd@jeffersoncountywi.gov

3.
REPORTS:

A. The CONTRACTOR agrees to timely submit reports as may be required by the COUNTY in its sole discretion.

B. All reports, studies, analyses, memoranda and related data and material developed during the performance of this Contract shall be submitted to and be the exclusive property of the COUNTY and the COUNTY shall have the right to use them for any purpose without any further compensation to the CONTRACTOR. All of the documents and materials prepared or assembled by the CONTRACTOR under this Contract will not be made available to any individual, agency, public body or organization other than the COUNTY unless legally required otherwise, at which point the CONTRACTOR is obligated to notify the COUNTY of the same in advance thereof.

C. The documents and materials prepared in whole or in part under this Contract shall not be made the subject of any report, book, writing or oral dissertation by the CONTRACTOR. If this Contract is terminated, all finished or unfinished documents or materials prepared under this Contract shall be immediately transmitted to the COUNTY upon termination.

4. TIME OF PERFORMANCE:

The services to be performed under this Contract are to be undertaken and completed in such sequence as to assure expeditious completion in light of the purpose of this Contract, but in any event all of the services required hereunder shall be completed as indicated on the top of Page 1 of this Contract under "Time of Performance," which is the termination date of this Contract. In addition to all other remedies available to the COUNTY, should the Contract not be completed by the date specified herein, the CONTRACTOR shall continue to be obligated thereafter to fulfill CONTRACTOR'S responsibility to complete the services and to execute any amendments to this Contract as deemed necessary by the COUNTY.

5. CONDITIONS OF PERFORMANCE AND COMPENSATION:

A. **Performance -** The CONTRACTOR agrees that its work shall conform to such recognized high professional standards as are prevalent in this field of endeavor and like services.

B. **Place of Performance –** The COUNTY shall determine the place or places where services shall be provided by the CONTRACTOR.

C. **Compensation -** The COUNTY agrees to pay, subject to the contingencies herein, and the CONTRACTOR agrees to accept for the satisfactory performance of the services under this Contract, the maximum as indicated on the top of Page 1 of this Contract under "Total Amount of Contract," inclusive of all expenses. In no event will the total compensation exceed the maximum amount indicated on the top of Page 1 of this Contract. Compensation for services provided under this Contract is contingent upon the approval process set forth in Section 3 of this Contract under "Specific Conditions of Payment." Section 66.0135, Wis. Stats., will apply to any late payments by the COUNTY, except as provided for by Section 22 of this Contract.

D. **Taxes, Social Security and Government Reporting -** Personal income tax payments, social security contributions and all other governmental reporting and contributions as a consequence of the CONTRACTOR receiving payment under this Contract shall be the sole responsibility of the CONTRACTOR.

E. **Subcontracting -** The CONTRACTOR shall not subcontract for the performance of any of the services set forth herein without prior written approval obtained from the COUNTY. If any work or service is subcontracted, it shall be specified by written contract or agreement and shall be subject to each provision of this Contract. The CONTRACTOR shall be as fully responsible to the COUNTY for the acts and omissions of his subcontractors and/or persons either directly or indirectly employed by him, as he is for the acts and omissions of persons directly employed by him.

6. INDEMNIFICATION AND DEFENSE OF SUITS:

The CONTRACTOR agrees to release, indemnify, defend, and hold harmless the COUNTY, its officials, officers, employees, and agents from and against all judgments, damages, penalties, losses, costs, claims, expenses, suits, demands, debts, actions and/or causes of action of any type or nature whatsoever, including actual and reasonable attorney fees, which may be sustained or to which they may be exposed, directly or indirectly, by reason of personal injury, death, property damage, or other liability, alleged or proven, resulting from or arising out of the performance under this agreement by CONTRACTOR, its officers, officials, employees, agents or assigns. The COUNTY does not waive, and specifically reserves, it's right to assert any and all affirmative defenses and limitations of liability as specifically set forth in Wisconsin Statutes, Chapter 893 and related statutes.

7. REGULATIONS:

CONTRACTOR agrees to comply with all of the requirements of all federal, state and local laws related thereto.

8. SAFETY REQUIREMENTS:

All material, equipment and supplies provided to the COUNTY must comply with all safety requirements as set forth by, among other provisions, the Wisconsin Administration Code, Rules of the Industrial Commission on Safety and all applicable OSHA standards.

9. VENUE AND APPLICABLE LAW:

Any lawsuits related to or arising out of disputes under this Contract shall be commenced and tried in the Circuit Court of Jefferson County, Wisconsin and the COUNTY and CONTRACTOR shall submit to the jurisdiction of the Circuit Court for such lawsuits. This Contract and any disputes arising under it shall be governed by the laws of the State of Wisconsin.

10. TERMINATION OF CONTRACT FOR CAUSE:

If through any cause, the CONTRACTOR shall fail to fulfill in a timely and proper manner its obligations under this Contract, or if the CONTRACTOR violates the covenants, agreements or stipulations of this

Contract, the COUNTY shall have the right to terminate this Contract by giving written notice, as provided for in Section 25 of this Contract, to the CONTRACTOR of such termination. The written notice shall be provided to the CONTRACTOR at least five (5) days before the effective date of such termination. The COUNTY, in its sole discretion, may allow the CONTRACTOR a reasonable amount of time to cure a breach of the terms of this Contract, if the COUNTY determines that the breach is amenable to a cure. The COUNTY shall not unreasonably withhold such permission. The COUNTY'S decision to allow the CONTRACTOR a reasonable amount of time to cure said breach in one instance does not constitutes a waiver of a subsequent breach of the same or any other term of this Contract, nor shall it be deemed to waive the need for further consent or approval from the COUNTY to cure any subsequent breaches, regardless of their nature.

In the event that this Contract is terminated for any reason by either party, all finished and unfinished documents, data, studies, surveys, drawings, maps, models, photographs, reports or other materials related to the services prepared by the CONTRACTOR under this Contract shall, at the option of the COUNTY, become the property of the COUNTY.

Notwithstanding the above, the CONTRACTOR shall not be relieved of liability to the COUNTY for damages sustained by the COUNTY by virtue of any breach of this Contract by the CONTRACTOR, and the COUNTY may withhold any payments due the CONTRACTOR for the purpose of set off until such time as the exact amount of damages due to the COUNTY from the CONTRACTOR is determined and recovered.

11. CHANGES:

All changes that are mutually agreed upon by and between the COUNTY and the CONTRACTOR, including any increase or decrease in the amount of the CONTRACTOR'S compensation, shall be in writing and designated as written amendments to be attached to this Contract.

12. WAIVER:

One or more waivers by any party of any term of this Contract will not be construed as a waiver of a subsequent breach of the same or any other term hereof. The consent or approval given by any party with respect to any act by the other party requiring such consent or approval shall not be deemed to waive the need for further consent or approval of any subsequent act by such party.

13. PERSONNEL:

A. The CONTRACTOR represents that it has or will secure, at its own expense, all personnel required in performing the services under this Contract. Such personnel shall not be employees of or have any contractual relationship with the COUNTY.

B. All of the services required hereunder will be performed by the CONTRACTOR or under its supervision and all personnel engaged in the work shall be fully qualified and shall be authorized or permitted under state and local law to perform such services.

14. ASSIGNMENT:

The CONTRACTOR shall not assign or transfer this Contract and shall not transfer any interest in it without the prior written consent of the COUNTY. Claims for money due or to become due to the CONTRACTOR from the COUNTY under this Contract may be assigned to a bank, trust company or other financial institution without COUNTY approval; however, notices, as provided for in Section 25 of this Contract, of any such assignment or transfer shall be furnished promptly to the COUNTY.

15. RECORDS:

A. **Establishment and Maintenance of Records -** Records shall be maintained by the CONTRACTOR with respect to all matters covered by this Contract. The records shall be maintained for a period of three (3) years after receipt of final payment under this Contract, except as otherwise authorized by Jefferson County Corporation Counsel.

B. **Documentation of Cost -** All costs of the CONTRACTOR shall be supported by properly executed payrolls, time records, invoices, contracts or vouchers, or other official documentation evidencing in proper detail the nature and propriety of other accounting documents pertaining in whole or in part to this Contract and shall be clearly identified and readily accessible.

16. AUDITS AND INSPECTIONS:

In the event that the COUNTY deems it necessary to conduct an audit or inspection, the CONTRACTOR shall, during normal business hours, furnish or make available at a time designated by the COUNTY and in the form required by the COUNTY, information, records and reports regarding powers, duties, activities, organization, property, financial transactions, method of operation, or any and all other records, reports or information in the CONTRACTOR'S custody or control as deemed pertinent by the COUNTY to this Contract.

The CONTRACTOR shall provide to the COUNTY'S inspectors or auditors access to all property, equipment and facilities in the CONTRACTOR'S custody or control as the inspectors or auditors deem related to the services provided or purchased under this Contract. The CONTRACTOR shall be expected to provide, at the CONTRACTOR'S expense, reasonable time by the CONTRACTOR'S personnel as may be required for the COUNTY'S inspectors or auditors to perform the inspection or audit.

Any information provided to the COUNTY'S inspectors or auditors which are deemed confidential by federal, state or local laws shall be held as confidential and not disclosed to the public unless legally required otherwise.

17. NON-DISCLOSURE:

For the purposes of this Contract, the parties agree to the following definitions.

Discloser: The term "Discloser" shall refer to the party or parties in a position to disclose to the other certain Sensitive and/or Confidential Information which is or must remain the property of the disclosing party.

Recipient: The term "Recipient" shall refer to the party or parties in a position to receive certain Sensitive and/or Confidential Information from the disclosing party that is not to be disclosed or used in violation hereof.

Sensitive and/or Confidential Information: The term "Confidential Information" as used herein means: (1) any Trade Secret of Discloser as defined in the Uniform Trade Secrets Act, Sec. 134.90, Wis. Stats. or any other applicable state or federal trade secrets law; and (2) any non-public information, documentation, and/or devices disclosed or made available by Discloser to Recipient in any form including, but not limited to, all data or know-how either created by Discloser or for Discloser, any information conveyed to Discloser by a third party to which Discloser is bound by a confidentiality agreement not to disclose, the whole or any portion of any technical, scientific, laboratory, experimental or research data, research and development information, information concerning equipment, designs, processes, procedures, formulae, recipes, improvements, customer lists, records, or engineering drawings, documentation and information about products, sales information, formulae, recipes, manufacturing techniques, processes, design of software or hardware, applications or systems, used or developed by Discloser, source codes, other information relating to computer programming, and any information used for the conduct of Discloser's business including, but not limited to, plans, programs, marketing, advertising, sales strategies, policies, costs, pricing, and other financial information.

Sensitive and/or Confidential Information shall also include but shall not be limited to:

- Confidential Information (business or personal) including copyrighted, trademarked or patented information;
- Electronic protected health information (ePHI) protected by Federal HIPAA legislation;
- Intellectual Property (IP);
- Credit card data regulated by the Payment Card Industry (PCI);
- Personal Identity Information (PII);
- Information relating to an ongoing criminal investigation;

- Court-ordered settlement agreements requiring non-disclosure;
- Information specifically identified by this Contract as restricted;
- Other information for which the degree of adverse effect that may result from unauthorized access or disclosure is high;

Whether in writing or not, which the Discloser discloses to Recipient, including, but not limited to, any information relating to the policies, procedures and administration of the Discloser, its affiliates' or customers' ongoing operations, and personnel. It is the intention of the parties in defining Sensitive and/or Confidential Information that any and all information which in any way relates to Discloser's operations, no matter what the nature thereof, which was disclosed by Discloser or which is developed by either party as part of their services in carrying out the Contract performance reference herein shall be and remain confidential pursuant to this Contract. This includes but is not limited to:

- Applications for services
- Account numbers or balances
- Payment histories
- Identity of customers
- Social Security numbers
- Credit reports or histories
- Any other financial information regarding Jefferson County or its customers
- The terms of this Contract
- HIPAA-related information

Sensitive and/or Confidential Information for purposes of this Contract does not include information that:

- Can be demonstrated to have been published or was otherwise in the public domain before disclosure by Discloser to Recipient;
- Can be demonstrated that, after its disclosure by Discloser to Recipient, is published, or otherwise comes into the public domain through no act or omission by Recipient, by a third party who has a legal right to do so;
- Recipient receives or has received from a third party who as a legal right to disclose it;
- Recipient has in written or physical embodiment form prior to disclosure by Discloser;
- Is independently developed by Recipient without reference to or reliance on Discloser's Sensitive and/or Confidential Information as evidenced by credible written evidence; and
- Becomes subject to the open records mandates of both federal and state law, including but not limited to, Wis. Stats. §§ 19.31 – 19.37.

A. **Acknowledgment of Confidential Relationship –** The County is required to ensure the confidentiality of any Sensitive and/or Confidential Information that the CONTRACTOR may have access to or become privy to under the state and federal laws including, but not limited to, HIPAA and the Wisconsin Privacy of Consumer Financial and Health Information, Wis. Admin. Code Ch. INS 25. The CONTRACTOR hereby acknowledges and agrees that any Sensitive and/or Confidential Information disclosed to it by the COUNTY is for the limited purpose of providing services and the CONTRACTOR will maintain the Confidential Information in confidence, and a confidential relationship will arise between the CONTRACTOR and the COUNTY by reason of such submission and/or disclosure. The CONTRACTOR further acknowledges and agrees that the Sensitive and/or Confidential Information of the COUNTY is proprietary to the COUNTY and that any unauthorized disclosure or unauthorized use as more fully set forth herein will cause harm and/or loss to the COUNTY.

B. **Use and Disclosure of Sensitive and/or Confidential Information.** The CONTRACTOR agrees neither to copy, sell, transfer, publish, disclose, display or otherwise use for its own benefit, nor to disclose to third parties, any Sensitive and/or Confidential Information whether from observation, from any materials submitted or from disclosures by the COUNTY hereunder. The CONTRACTOR further agrees neither to make nor retain any copies of nor directly or indirectly use any process or other proprietary information disclosed to it or any process deceptively similar thereto without the COUNTY'S prior written approval, which the COUNTY may withhold in its sole discretion. In no event shall either party use Sensitive and/or Confidential Information in

a way, which violates local, state or federal laws. The duty to protect Sensitive and/or Confidential Information shall survive the termination of this Contract and shall be subject to the open records provisions of both state and federal law.

The CONTRACTOR shall instruct its employees, agents and contractors of their obligations under this Contract and instruct them to use the same care and discretion with respect to the Sensitive and/or Confidential Information as the CONTRACTOR is obligated to use and to not circumvent any security procedures or devices with respect to Sensitive and/or Confidential Information.

C. **Title remains with the COUNTY.** All innovations, inventions, devices, processes and/or formulas developed by the CONTRACTOR for the COUNTY shall be deemed to be the sole property of the COUNTY. The CONTRACTOR agrees to disclose in writing to the COUNTY any and all formulas, ingredient specifications and descriptions, processing methods, items, ideas or concepts which are directly related to work performed by the CONTRACTOR on behalf of the COUNTY which constitute innovations or inventions developed by the CONTRACTOR either solely or jointly in connection with work performed by the CONTRACTOR at the request of or under any assignment by the COUNTY. The CONTRACTOR also agrees to assign to the COUNTY any and all interest it may have in such inventions or innovations.

D. **Indemnification by the CONTRACTOR**. The CONTRACTOR agrees to take precautions to avoid wrongful disclosures or use of Confidential Information and will indemnify the COUNTY and hold the COUNTY harmless from all losses; expenses, including reasonable attorney's fees; or liability arising from or in connection with such unauthorized use or disclosure. In addition, the CONTRACTOR acknowledges that in the event of a breach or threatened breach of this Contract, irreparable damage will immediately occur to the COUNTY and the CONTRACTOR will indemnify the COUNTY from all losses, liabilities, and expenses, including reasonable attorney's fees, incurred by the COUNTY as a result thereof.

E. **Duty of Inquire.** If either party has a question concerning whether information qualifies as Sensitive and/or Confidential Information under this Contract, each shall have a duty to inquire whether the information is deemed sensitive and/or confidential before taking any action contrary to this Contract.

For COUNTY inquire to:
Corporation Counsel
(920) 674-7136

For CONTRACTOR inquire to:

F. **Duty to Safeguard.** Each party shall take all reasonable steps to safeguard any and all Sensitive and/or Confidential Information in their possession. Each party shall ensure, to the extent possible, that access to Sensitive and/or Confidential Information is restricted only to properly authorized employees, agents, officers and/or subcontractors and shall take measures to protect the security of any documentation or computer containing Sensitive and/or Confidential Information.

18. CONFLICT OF INTEREST:

A. **Interest in Contract -** No officer, employee or agent of the COUNTY who exercises any functions or responsibilities in connection with the carrying out of any services or requirements to which this Contract pertains, shall have any personal interest, direct or indirect in this Contract.

B. **Interest of Other Local Public Officials -** No member of the governing body of the locality, who exercises any functions of responsibilities in the review or approval of the carrying out of this Contract, shall have any personal interest, direct or indirect, in this Contract.

C. **Interest of Contractor and Employees -** If the CONTRACTOR is aware or becomes aware that any person described in Sections 20, A. and B. of this Contract has any personal financial interest, direct or indirect, in this Contract, the CONTRACTOR shall immediately disclose such knowledge to the COUNTY. The CONTRACTOR further covenants that it presently has no interest and shall not acquire any interest, direct or indirect, which would conflict in any manner or degree with the performance of its services hereunder. The CONTRACTOR further covenants that in the performance of this Contract no person having any conflicting interest shall be employed or subcontracted.

19. DISCRIMINATION PROHIBITED:

A. The CONTRACTOR shall not discriminate against any individual on the basis of age, race, creed, color, disability, marital status, sex, national origin, ancestry, membership in the National Guard, state defense force or any reserve component of the military forces of the United States or this state. The CONTRACTOR may refuse to employ individuals based on conviction and arrest records only as allowed by Sec. 111.335, Wis. Stats.

B. The CONTRACTOR will cause the foregoing provisions to be inserted into all subcontracts, if any, for any work covered by this Contract so that such provision will be binding upon each subcontractor, provided that the foregoing provisions shall not apply to contracts or subcontracts for standard commercial supplies or raw materials.

20. INSURANCE:

A. The CONTRACTOR shall be solely responsible to meet the CONTRACTOR'S insurance needs as required by the COUNTY during the terms of this Contract or any extension thereof.

B. The Certificate(s) of Insurance shall be issued by a company or companies authorized to do business in the State of Wisconsin and satisfactory to the COUNTY. Such insurance should be primary. The CONTRACTOR shall furnish the COUNTY with a certificate of insurance and upon request, certified copies of the required insurance policies. The certificate(s) shall reference the Contract and name Jefferson County, its boards, commissions, agencies, officers, employees and representatives as additional insureds and provide for thirty (30) days advance notice, as provided for in Section 25 of this Contract, of any change, cancellation or non-renewal during the term of this Contract.

C. The CONTRACTOR shall not allow subcontractors, if any, to commence work until the aforementioned documents, where applicable, have been obtained from the subcontractor(s) and approved by the COUNTY.

D. No payments or disbursements under this Contract shall be made if such proof has not been furnished to the COUNTY. Failure to submit an insurance certificate, as required, can make this Contract void at the COUNTY'S discretion.

21. FORCE MAJEURE:

A. If the performance of any part of this Contract by the CONTRACTOR is delayed or rendered impossible by reason of natural disaster, flood, fire, riot, explosion, war or actions or decrees of governmental bodies, the CONTRACTOR shall immediately give notice, as provided for in Section 25 of this Contract, to the COUNTY of the nature of such conditions and the extent of delay and shall do everything possible to resume performance. If the period of nonperformance exceeds twenty-one (21) days from the receipt of said notice of the Force Majeure Event, the COUNTY may, by giving written notice as provided for in Section 25 of this Contract, terminate this Contract.

B. If the ability of the COUNTY to compensate the CONTRACTOR is delayed by reason of natural disaster, flood, fire, riot, explosion, war or actions or decrees of governmental bodies, the COUNTY shall immediately give notice, as provided for in Section 25 of this Contract, to the CONTRACTOR of the nature of such conditions and the expected date that compensation will be made. Section 66.0135, Wis. Stats., shall not apply to any late payment by the COUNTY due to circumstances under this Subsection B.

22. OTHER PROVISIONS:

A. **Publicity Releases –** The CONTRACTOR agrees not to refer to award of this Contract in commercial advertising in such a manner that states or implies that the products or services provided are endorsed or preferred by the COUNTY.

B. **Appropriation of Funds** – This Contract is contingent upon annual authorization of funding by the COUNTY governing body. In the event funding is not approved or is terminated, the COUNTY may terminate this Contract by providing forty-five (45) days written notice to the CONTRACTOR.

C. **Severability** -- In the event that any of the provisions of this Contract are deemed invalid or unenforceable, the remaining provisions shall be construed and enforced as if such invalid or unenforceable provisions were not contained herein.

D. **Independent Contractor Status -** This Contract does not in any way create the relationship of joint venture, partnership, principal, or employer/employee between the CONTRACTOR and the COUNTY, their agents, employees, subcontractors, officers and/or representatives. The CONTRACTOR, its employees, agents, subcontractors, and/or representatives shall not act or attempt to act, or represent itself, directly or by implication, as an agent for the COUNTY or in any manner assume any obligation on behalf of or in the name of the COUNTY.

23. NOTICES:

Any and all notices shall be in writing and deemed served upon depositing same with the United States Postal Service as "Certified Mail, Return Receipt Requested", addressed to the CONTRACTOR at:

And to the COUNTY at: Jefferson County Finance
311 S Center Ave-Room 109
Jefferson, WI 53549

All other correspondence shall be addressed as above, but may be sent by "Regular Mail" and deemed delivered upon receipt by the addressee.

JEFFERSON COUNTY FINANCE Marc DeVries, CPA, Finance Director Signature:_____ Date:_____ **JEFFERSON COUNTY CORPORATION COUNSEL** Blair Ward, Corporation Counsel Signature:_____ Date: _____	PROVIDER (To be signed by the person authorized to legally bind your firm to this Contract.) Firm: _____ Address: _____ City/State: _____ Zip Code: _____ Printed Name: _____ Signed Name: _____ (Required) Title: _____ Date: _____

JEFFERSON COUNTY ADMINISTRATION Benjamin Wehmeier, County Administrator Signature:_____ Date: _____	**Distribution**: Original – Purchasing Copy – Provider(s) Copy – Responsible Department(s)

DEPARTMENT OF HEALTH SERVICES **STATE OF WISCONSIN**
Division of Enterprise Services
F-00759 (01/2018)

Contract Name: Enter Text
Contract Number: Enter text

BUSINESS ASSOCIATE AGREEMENT
With Contract

This Business Associate Agreement is incorporated into the Underlying Contract known as Enter Text and is made between the Wisconsin Department of Health Services, Enter Text ("Covered Entity"), and the Enter text ("Business Associate"), collectively the "Parties."

This Agreement is specific to those services, activities, or functions performed by the Business Associate on behalf of the Covered Entity when such services, activities, or functions are covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), including all pertinent regulations (45 CFR Parts 160 and 164) issued by the U.S. Department of Health and Human Services. Services, activities, or functions covered by this Agreement include, but are not limited to:

Describe Services/Functions

The Covered Entity and Business Associate agree to modify the Contract to incorporate the terms of this Agreement and to comply with the requirements of HIPAA addressing confidentiality, security, and the transmission of individually identifiable health information created, used, or maintained by the Business Associate during the performance of the Contract and after Contract termination. The parties agree that any conflict between provisions of the Contract and the Agreement will be governed by the terms of the Agreement.

1. DEFINITIONS

The following terms used in this Agreement shall have the same meaning as those terms in the HIPAA Rules: Breach, Data Aggregation, Designated Record Set, Disclosure, Health Care Operations, Individual, Minimum Necessary, Notice of Privacy Practices, Protected Health Information, Required by Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use.

Specific Definitions:

a. Business Associate: "Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103 and, in reference to the party to this Agreement, shall mean Enter text.

b. Covered Entity: "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103 and, in reference to the party in this Agreement, shall mean the Wisconsin Department of Health Services.

c. HIPAA Rules: "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

2. RESPONSIBILITIES OF BUSINESS ASSOCIATE

a. Business Associate shall not use or disclose any Protected Health Information except as permitted or required by the Agreement, as permitted or required by law, or as otherwise authorized in writing by the Covered Entity, if done by the Covered Entity. Unless otherwise limited herein, Business Associate may use or disclose Protected Health Information for Business Associate's proper management and administrative services, to carry out legal responsibilities of Business Associate, and to provide data aggregation services relating to health care operations of the Covered Entity if required under the Agreement. Business Associate is not authorized to create de-identified information from PHI.

b. Business Associate shall not request, use, or disclose more than the minimum amount of Protected Health Information necessary to accomplish the purpose of the use or disclosure.

c. Business Associate shall inform the Covered Entity if it or its subcontractors will perform any work outside the U.S. that involves access to, or the disclosure of, Protected Health Information.

3. SAFEGUARDING AND SECURITY OF PROTECTED HEALTH INFORMATION

a. Business Associate shall use appropriate safeguards, including complying with Subpart C of 45 CFR Part 164 with respect to electronic Protected Health Information, to prevent use or disclosure of Protected Health Information other than as provided for by the Agreement.

b. Business Associate shall cooperate in good faith in response to any reasonable requests from the Covered Entity to discuss, review, inspect, and/or audit Business Associate's safeguards.

4. REPORTING OF A VIOLATION TO COVERED ENTITY BY BUSINESS ASSOCIATE

The Business Associate shall report to Covered Entity any use or disclosure of Protected Health Information not provided for by the Agreement of which it becomes aware, including breaches of unsecured Protected Health Information as required at 45 CFR 164.410 and any successful security incident which it becomes aware of.

a. **Discovery of a Violation**. The Business Associate must inform the Covered Entity by telephone call, plus email or fax, within five business days following the discovery of any violation.

   i. The Violation shall be treated as "discovered" as of the first day on which the Violation is known to the Business Associate or, by exercising reasonable diligence would have been known to the Business Associate.
   ii. Notification shall be provided to one of the contact persons as listed in section 4.d.
   iii. Notification shall occur within five business days that follows discovery of the Violation.

b. **Mitigation.** The Business Associate shall take immediate steps to mitigate any harmful effects of the unauthorized use, disclosure, or loss. The Business Associate shall reasonably cooperate with the Covered Entity's efforts to seek appropriate injunctive relief or otherwise prevent or curtail such threatened or actual breach, or to recover its Protected Health Information, including complying with a reasonable Corrective Action Plan.

c. **Investigation of Breach**. The Business Associate shall immediately investigate the Violation and report in writing within ten days to a contact listed in section 4.d. with the following information:

   i. Each Individual whose Protected Health Information has been or is reasonably to have been accessed, acquired, or disclosed during the Incident;
   ii. A description of the types of Protected Health Information that were involved in the Violation (such as full name, social security number, date of birth, home address, account number);
   iii. A description of unauthorized persons known or reasonably believed to have improperly used or disclosed Protected Health Information or confidential data;
   iv. A description of where the Protected Health Information or confidential data is believed to have been improperly transmitted, sent, or utilized;
   v. A description of probable causes of the improper use or disclosure;
   vi. A brief description of what the Business Associate is doing to investigate the Incident, to mitigate losses, and to protect against further Violations;
   vii. The actions the Business Associate has undertaken or will undertake to mitigate any harmful effect of the occurrence; and
   viii. A Corrective Action Plan that includes the steps the Business Associate has taken or shall take to prevent future similar Violations.

d. **Covered Entity Contact Information.** To direct communications to above-referenced Covered Entity's staff, the Business Associate shall initiate contact as indicated herein. The Covered Entity reserves the right to make changes to the contact information by giving written notice to the Business Associate.

DHS Program Manager:
Name of DHS Contact
Address
Phone Number
Email Address

DHS Privacy Officer:
c/o Office of Legal Counsel
Department of Health Services
1 W. Wilson Street
Madison, WI 53707
608-266-5484

DHS Security Officer:
Department of Health Services
1 W. Wilson Street
Madison, WI 53707
608-261-8310

5. USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION BY SUBCONTRACTORS OF THE BUSINESS ASSOCIATE

In accordance with 45 CFR 164.502(e)(1) and 164.308(b), if applicable, the Business Associate shall ensure that any subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information.

6. COMPLIANCE WITH ELECTRONIC TRANSACTIONS AND CODE SET STANDARDS

If the Business Associate conducts any Standard Transaction for, or on behalf of, a Covered Entity, the Business Associate shall comply, and shall require any subcontractor or agent conducting such Standard Transaction to comply, with each applicable requirement of Title 45, Part 162, of the Code of Federal Regulation. The Business Associate shall not enter into, or permit its subcontractors or agents to enter into, any Agreement in connection with the conduct of Standard Transactions for, or on behalf of, Covered Entity that:

a. Changes the definition, Health Information condition, or use of a Health Information element or segment in a Standard;
b. Adds any Health Information elements or segments to the maximum defined Health Information Set;
c. Uses any code or Health Information elements that are either marked “not used” in the Standard’s Implementation Specification(s) or are not in the Standard’s Implementation Specifications(s); or
d. Changes the meaning or intent of the Standard’s Implementations Specification(s).

7. ACCESS TO PROTECTED HEALTH INFORMATION

At the direction of the Covered Entity, the Business Associate agrees to provide access, in accordance with 45 CFR 164.524, to any Protected Health Information held by the Business Associate, which Covered Entity has determined to be part of Covered Entity’s Designated Record Set, in the time and manner designated by the Covered Entity. This access will be provided to Covered Entity, or (as directed by Covered Entity) to an Individual, in order to meet requirements under the Privacy Rule.

8. AMENDMENT OR CORRECTION TO PROTECTED HEALTH INFORMATION

At the direction of the Covered Entity, the Business Associate agrees to amend or correct Protected Health Information held by the Business Associate, which the Covered Entity has determined is part of the Covered Entity’s Designated Record Set, in the time and manner designated by the Covered Entity in accordance with 45 CFR 164.526.

9. DOCUMENTATION OF DISCLOSURES OF PROTECTED HEALTH INFORMATION BY THE BUSINESS ASSOCIATE

The Business Associate agrees to document and make available to the Covered Entity, or (at the direction of the Covered Entity) to an Individual, such disclosures of Protected Health Information to respond to a proper request by the Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

10. INTERNAL PRACTICES

The Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of Protected Health Information available to the federal Secretary of Health and Human Services (HHS) in a time and manner determined by the HHS Secretary, or designee, for purposes of determining compliance with the requirements of HIPAA.

11. TERM AND TERMINATION OF AGREEMENT

a. The Business Associate agrees that if in good faith the Covered Entity determines that the Business Associate has materially breached any of its obligations under this Agreement, the Covered Entity may:

    i. Exercise any of its rights to reports, access, and inspection under this Agreement;
    ii. Require the Business Associate within a 30-day period to cure the breach or end the violation;

iii. Terminate this Agreement if the Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity;
iv. Immediately terminate this Agreement if the Business Associate has breached a material term of this Agreement and cure is not possible.

b. Before exercising either 11.a.ii. or 11.a.iii, the Covered Entity will provide written notice of preliminary determination to the Business Associate describing the violation and the action the Covered Entity intends to take.

12. RETURN OR DESTRUCTION OF PROTECTED HEALTH INFORMATION

Upon termination, cancellation, expiration, or other conclusion of this Agreement, the Business Associate will:

a. Return to the Covered Entity or, if return is not feasible, destroy all Protected Health Information and any compilation of Protected Health Information in any media or form. The Business Associate agrees to ensure that this provision also applies to Protected Health Information of the Covered Entity in possession of subcontractors and agents of the Business Associate. The Business Associate agrees that any original record or copy of Protected Health Information in any media is included in and covered by this provision, as well as all originals or copies of Protected Health Information provided to subcontractors or agents of the Business Associate. The Business Associate agrees to complete the return or destruction as promptly as possible, but not more than **30** business days after the conclusion of this Agreement. The Business Associate will provide written documentation evidencing that return or destruction of all Protected Health Information has been completed.

b. If the Business Associate destroys Protected Health Information, it shall be done with the use of technology or methodology that renders the Protected Health Information unusable, unreadable, or undecipherable to unauthorized individuals as specified by HHS in HHS guidance. Acceptable methods for destroying Protected Health Information include:

i. For paper, film, or other hard copy media: shredding or destroying in order that Protected Health Information cannot be read or reconstructed and
ii. For electronic media: clearing, purging, or destroying consistent with the standards of the National Institute of Standards and Technology (NIST).

Redaction is specifically excluded as a method of destruction of Protected Health Information unless the information is properly redacted so as to be fully de-identified.

c. If the Business Associate believes that the return or destruction of Protected Health Information is not feasible, the Business Associate shall provide written notification of the conditions that make return or destruction not feasible. If the Business Associate determines that return or destruction of Protected Health Information is not feasible, the Business Associate shall extend the protections of this Agreement to Protected Health Information and prohibit further uses or disclosures of the Protected Health Information of the Covered Entity without the express written authorization of the Covered Entity. Subsequent use or disclosure of any Protected Health Information subject to this provision will be limited to the use or disclosure that makes return or destruction not feasible.

13. COMPLIANCE WITH STATE LAW

The Business Associate acknowledges that Protected Health Information from the Covered Entity may be subject to state confidentiality laws. Business Associate shall comply with the more restrictive protection requirements between state and federal law for the protection of Protected Health Information.

14. MISCELLANEOUS PROVISIONS

a. **Indemnification for Breach**. Business Associate shall, to the extent allowed by Wisconsin law, indemnify the Covered Entity for costs associated with any Incident arising from the acquisition, access, use, or disclosure of Protected Health Information by the Business Associate in a manner not permitted under HIPAA Rules.

b. **Owner of PHI**. Under no circumtances shall Business Associate be deemed in any respect to be owner of any PHI created or received by Business Associate on behalf of Covered Entity.

c. **Third Party Rights**. The terms of this Agreement do not grant any rights to any parties other than Business Associate and Covered Entity.

d. **Independent Contractor Status**. For the purposes of this Agreement, Business Associate is an independent contractor of Covered entity and shall not be considered an agent of Covered Entity.

e. **Automatic Amendment**. This Agreement shall automatically incorporate any change or modification of applicable state or federal law as of the effective date of the change or modification. The Business Associate agrees to maintain compliance with all changes or modifications to applicable state or federal law.

f. **Interpretation of Terms or Conditions of Agreement**. Any ambiguity in this Agreement shall be construed and resolved in favor of a meaning that permits the Covered Entity and Business Associate to comply with applicable state and federal law.

g. **Survival**. All terms of this Agreement that by their language or nature would survive the termination or other conclusion of this Agreement shall survive.

IN WITNESS WHEREOF, the undersigned have caused this Agreement to be duly executed by their respective representatives.

COVERED ENTITY		BUSINESS ASSOCIATE	
Print Name:	Enter text	Print Name:	Enter text
SIGNATURE:		**SIGNATURE:**	
Title:	Enter text	Title:	Enter text
Date:	Choose date	Date:	Choose date

COVERED ENTITY	
Print Name:	Enter text
SIGNATURE:	
Title:	Enter text
Date:	Choose date

HR0410 **COMPUTER, INTERNET, AND TELEPHONE USE.**

Jefferson County provides employees and other authorized Users with access to, and the use of, a variety of information technology resources. These resources are provided in an effort to allow employees and other authorized Users to be more efficient, productive, and to have access to information that is necessary to carry out responsibilities of the County. All are expected and required to use these information technology resources in a manner consistent with position and work responsibilities in a professional, lawful and ethical manner that will reflect positively on themselves and Jefferson County. Those not assigned access to and use of information technology resources are expected and required to review and acknowledge with signature the same policies as those who have been assigned direct use.

All data, communications, and information transmitted, maintained or stored by government authority on Jefferson County information technology resources is subject to the State of Wisconsin Public Records Law, state and federal confidentiality laws and privacy standards, including protection of personal information collected on its citizens. The confidentiality, integrity, accessibility, retention, and disclosure of said information shall be governed by applicable law, and policies adopted by the County, including contextual information and file history generated automatically by computer operating systems or software programs.

Jefferson County Management Information Systems (MIS) has made a commitment to follow the concept of "Green IT": responsible ordering to reduce waste; secure recycling of information technology resources taken off inventory; recycled paper and toner cartridges wherever feasible; encouraging employees and other authorized Users to turn off screen monitors at the end-of–the day and to shutdown computers on non-software-update nights; and other industry-recommended, environmentally-friendly practices.

The Computer, Internet, and Telephone Use Ordinance may be modified at any time to reflect changes in technology, strategic direction or for any other reason deemed sufficient by MIS. Distribution of the Personnel Policy which includes this Ordinance is to follow standard Human Resources Department procedure, including posting to the Jefferson County Employee and Public Websites. Additional distribution will be via the means deemed appropriate by MIS. Department-specific information technology resource use policies and procedures will be subject to MIS agreement and shall support the intent of this Ordinance. Training on the Ordinance shall begin at employee and other authorized User Orientation and further reinforced on-site as other policies and procedures are explained. Additional guidance on an as-needed basis on the Ordinance, specific software and hardware applications and the use of information technology resources, will be communicated to Users by MIS in the manner considered most efficient and cost effective.

Initiation of Departmental or County-wide Business Continuity or Disaster Recovery Plans may defer but not permanently override security and confidentiality practices as outlined in this Computer, Internet and Telephone Use Ordinance.

The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive, sexually explicit, and inappropriate material. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an email address on the Internet may lead to receipt of unsolicited email containing offensive content. Users accessing the Internet do so at their own risk. Jefferson County is not responsible for material viewed or downloaded by Users from the Internet.

To minimize risks and to encourage acceptable practice, use of the Internet and Information Technology Resources at Jefferson County is governed by the following policy:

A. **PERMITTED USE OF JEFFERSON COUNTY INTERNET, COMPUTERS AND TELEPHONES.**

1. For the purposes of this policy, the County will define "Information Technology Resources" as any equipment, hardware, software or telephone that is assigned and available for employees and other authorized Users to use in the course of Jefferson County employment or service. "Employee" is defined as all regular full-time, regular or occasional part-time, limited term employees, contracted employees, seasonal employees, State of Wisconsin employees working within County government, and volunteers. "Other Authorized Users" refers to County board members, students, contracted agents and consultants, researchers with documented approval from an Institutional Review Board (IRB), contracted private agency partnering with a county department, others as specified by County policy, and others granted authorization by MIS to access County-owned Information Technology Resources. Additionally, certain "Teleworkers" have been granted authorization from MIS to utilize home-based, outside-of-County buildings information technology resources. The term "User" is written interchangeably with the phrase "Employee and Other Authorized Users" throughout this Ordinance.
2. The computer, telephone, and network are the property of Jefferson County and are to be used for legitimate business purposes. Email generated is considered a legal, business document and subject to the same legal and business rules as any other document. Users are provided access to the computer network to assist in the performance of their duties. Other authorized Users may also be provided with access to the Internet through the computer network. All Users have a responsibility to use Jefferson County's computer resources and the Internet in a professional, lawful and ethical manner. Occasional limited appropriate personal use of the computer and/or telephone is permitted if approved by the Department Head and such use does not:
    a. Interfere with the User's or any employee's job performance;
    b. Have an undue effect on the computer or telephone system or Jefferson County network's performance;
    c. Violate any other policies, provisions, or guidelines applicable to the Jefferson County employee or other authorized User.
    d. Further, Users are responsible for the professional, ethical and lawful use of the computer and telephone system at all times. Personal use of the computer and telephone is a privilege that may be revoked at any time. Loss of email, Internet access or Jefferson County computer or privileges, telephone privileges, sanctions or other actions up to and including termination may be imposed for failure to follow this policy.
3. **Damage, Theft or Loss of County Property**. With use comes the responsibility to take care of County-owned property. While damage due to normal use over time can be expected, any non-typical damage (for example, fluid spilled on the computer) that may affect should be reported when it happens. The theft or loss (either by a User or unauthorized intruder) of County property must be reported to MIS immediately when detected. MIS will pursue every theft or loss as a security breach. The steps to "mitigate" (take action post-event to locate, restore usability, and notify individuals affected who are

covered by the State of Wisconsin "Notice of unauthorized acquisition of personal information" – the state's breach notification law) will depend on the extent of involvement. Additional information is found in the next section if the event involves a Portable Device (especially if outside of normal County business hours or off-County property). Users will be expected to cooperate with the investigation and mitigation process.

4. **Portable Devices**. An employee or authorized User with MIS approval may have access to portable devices for County business, including County-owned notebook; cellular telephone, Personal Digital Assistant (PDA); Smart Phone, Blackberry, Universal Serial Bus (USB); Flash Drive; Memory Stick; Jump Drive; Floppy Disk, Computer Disk (CD); Digital Video Disk (DVD); Backup Media; Smart Card and Tags; Radio Frequency Identification (RFID), Global Positioning System (GPS) and Remote Access Device (including security hardware).
   a. Security guidelines in the form of policies and procedures set by MIS must be followed, including: **Do not post, share or enter** without awareness of who around you may see the log-on ID and password screen (especially at any public location such as a hotel, airport kiosk, coffee shop, etc.); **Do not disable** the set timeout feature or protective software, such as encryption; **Do not load** unauthorized software; **Do not use** anyone else's or home-based equipment for County business unless authorized by MIS; **Do not remove or cover** the identifying label affixed by MIS; **Do not leave** the device unattended, including when information is on the screen. **Do be careful discussing confidential matters loudly** over the telephone in a public area or parking lot without being aware of who may be listening; **Do connect the notebook** to the network for protective software updates at least bi-weekly and when directed by MIS staff; **Use the device assigned to you**, keeping it in the storage case or attached to the lanyard provided; **Secure** the portable device off-site, including from damage due to weather conditions and when not in your personal possession; **Delete** data from a portable device immediately after downloading onto a County-located computer.
   b. **IN THE EVENT OF THE THEFT OR LOSS OF ANY PORTABLE DEVICE.** Contact MIS immediately. If unable to reach MIS staff through the county telephone directory during normal business hours, the MIS on-call cell phone number is 920-723-3040. Once in contact with an MIS employee, follow the instructions given to facilitate location of the device and secure any other equipment. If a cellular telephone or PDA is lost or stolen, occasionally its contents can be erased remotely. This prevents an attacker from obtaining any information from the device. The availability of this service depends on the capabilities of the product and the company providing network services for the product. Employees and other authorized Users with equipment so enabled should work with MIS staff to initiate erasure. Action needs to be taken as soon as possible to reduce loss of County information and equipment. The User must be prepared upon return to the office to cooperate with the investigation and mitigation process. Damage to a Portable Device as described in the previous section on Damage, Theft and Loss that does

not involve a security breach may be reported to MIS as soon as possible after return.

5. **Other Approved User or Inter-Network Connection, with Corresponding Information Technology Needs**. As listed in the Ordinance definition, an "Other Approved User" falls into a category of not being an "Employee" but having a contractual relationship with the County and need for information technology resource access.
   a. MIS will evaluate the feasibility of connecting the County network to any other network, whether private (for example, the County nursing home to a hospital) or government (for example, a state-required reporting system). This will include compatibility of the connection and the equipment and software (whether County owned or purchased or supplied by the other party). Approved connections are to be used only for the purpose intended. Any changes suggested by the other party after the initial connection has been made are to be reported immediately to MIS for review as to the influence on the County's network, need for updating of security policies and anti-threat protections, and budget impact.
   b. MIS will evaluate the information technology resources required for any party listed in the definition of "Other Authorized User", including electronic mailbox setup, county vs. the agent's computer equipment, and access levels including to proprietary software.
6. **Email**. While the use of email as a communication tool is becoming increasingly widespread, the issues surrounding its use are complex and not easily resolved.
   a. To ensure appropriate business use, as well as safeguarding the confidentiality of the information contained in emails, employees and other authorized Users must utilize organizational applications for email communications when carrying out job duties. The use of external email applications (e.g., Yahoo, Hotmail, etc.) is cautioned against due to potential concerns addressing protection of privacy, security threats and harm from malicious viruses, worms and other forms of attack.
   b. Transmission over the County's own network may be managed with internal controls such as unique User ID and authentication, policies and procedures, education, sanctions and physical controls such as a separate email account for a designated purpose. However with transmissions over a public or open network such as wireless Internet, the County's internal controls are no longer relevant.
   c. Do not store emails on non-County equipment off-site. Employees are reminded that an email becomes public record under the State of Wisconsin Public Records Law unless it is within one of the law's exceptions, in which case the record would be covered by the laws(s) governing that exception
   d. Users are cautioned to take care when composing the subject line in the header to minimize confidential information visible in the recipient's "Inbox"; Altering and storing of multiple versions of an email regarding strategic County business; and Checking the address in the "To", "Cc" prior to clicking "Send" to prevent a misdirected email or a "Reply to All" when only "Reply' should have been selected.

7. **Encryption.** Encryption is a process that transforms information into another form that offers a strong assurance, even if intercepted, lost or stolen, cannot be read by unauthorized users. Encryption where feasible can be a very important part of network, email and portable device security.
   a. MIS will assess the risk to County information technology resources and the need for encryption. Users must follow instructions to maintain encryption where implemented, and not remove or disable it.
   b. Encryption may be required by outside users; for example, emailing to an address that requires encryption or assigning a password to an attachment. Users should follow the directions as given by the requiring party, except that under no circumstance should a County User ID or password be revealed. Instead, decide on a temporary solution for this purpose only, with care taken when composing the reply email, without the word "password", which may flag the email when in transit by an online intruder scanning electronic mail messages. If questions or problems are encountered, notify MIS.
8. **Wireless Network Security.** Wireless is based on a shared medium. Because wireless communications work by radio wave, anyone properly equipped can intercept a wireless transmission. MIS has setup an infrastructure architecture in which all units communicate with one unit that connects to a wired network. Wireless access points (WAPs) provide an interface between the physical network and the various computers containing wireless cards. Infrastructure architecture improves security and performance because MIS can monitor central login points to detect illicit access attempts. It is important not to tamper with the physical equipment and wireless cards installed by MIS.
   a. Wireless connections are available in select County buildings, meant for Users with a MIS-installed wireless card. Any attempt at access by a "non-approved user" must be reported to the MIS Information Technology Manager or HIPAA Officer or the MIS Senior Microcomputer Specialist immediately (see also steps under "**IN THE EVENT OF THE THEFT OR LOSS OF ANY PORTABLE DEVICE**" listed previously in this Ordinance).
   b. Pockets of wireless connections just outside of County facilities have been discovered. It is impossible to know if these links are as safe and reliable as MIS-installed connections for sensitive county business. For this reason, it is highly recommended that within MIS facilities only County-installed connections be accessed.

B. **COMPUTER NETWORK USE LIMITATIONS.** Prohibited Activities. Without prior written permission from MIS, Jefferson County computers, telephones and network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, Trojan horse programs, security cracking-avoidance tools, etc.) or any other unauthorized materials.

C. **UNACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES**. Unacceptable uses of the County's Information Technology Resources include, but are not limited to, the following:

1. Unauthorized use.
2. Illegal purposes
3. Transmittal of threatening, abusive, obscene, lewd, profane or harassing material or material which suggests any lewd or lascivious act.
4. Inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference; material containing abusive, profane or offensive language, solicitation of non-County business, internet or email usage for personal gain, illegal activity, or any usage contrary to Jefferson County's best interest.
5. Intentionally preventing or attempting to prevent the disclosure of identity with the intent to frighten, intimidate, threaten abuse or harass another person.
6. Transmittal of material which is confidential to the County.
7. Disruption of network services, such as distributing computer viruses.
8. Use of someone else's identity and password for access to information technology resources without proper authorization.
9. Attempt to evade, disable or "crack" a password or User ID, remove the "Sign-On Banner" regarding network monitoring, delete the email disclaimer on out-going email, or other security provisions of systems on the network or a portable device.
10. Reproduction and/or distribution of copyrighted materials without appropriate authorization. Users may not illegally copy material protected under copyright law or make that material available to others for copying. Each employee and other authorized User is responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material the User wishes to download or copy. The employee and other authorized User may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of MIS.
11. Communicating official County business by "instant (text) messaging" on telephones. The paper trail created is on the cellular telephone bill only, without a report to keep as a permanent file record. Abbreviations used to quickly text may not be standard and difficult in the future to decipher. Text messages inadvertently received as a "wrong number" on a County-owned cellular telephone may need to be "opened" prior to deleting.
12. Intentionally ignoring notification of "Spam Quarantine" emails. The service is provided to prevent an important email from being missed. MIS will take responsibility to choose a product that best accommodates the needs of the County and is easy to use.

D. **SOFTWARE LIMITATIONS/EQUIPMENT MOVES.**

1. **Installations.** Only legal software may be installed on Jefferson County equipment. Software is considered legal if a software publisher has granted a right (or license) to Jefferson County to use one or more copies of its software and Jefferson County prohibits further copying and distribution of that software to others. All software installed on the Jefferson County network, Personal Computers (PCs), and other related devices must be authorized and approved by MIS. If the employee or other authorized User buys software, MIS must approve the purchase ahead of time. A copy of the Purchase Order and a copy of the license agreement must be provided to MIS before the software may be purchased. **Personal software installed on any County equipment is not allowed**. No software should be downloaded off the Internet to the network or installed on County equipment without the assistance of MIS to ensure proper licensing. Jefferson County equipment is any piece of hardware, software, firmware, notebook, personal computer (PC), Personal Data Assistant (PDA), telephony, or any other item purchased with Jefferson County funds. **Only MIS staff or department contact is allowed to install any software, hardware or firmware, including upgrades, on the Jefferson County network or Jefferson County equipment.**
2. **Moving.** Written requests for department computer equipment moves should be sent to MIS at least five days before the move is anticipated. Upon receipt of request, MIS staff will make arrangements to move or relocate equipment. Equipment, including telephones and computers, shall not be moved without MIS authorization. It is important not to move telephones around in the buildings without obtaining proper authorization from MIS because telephones are assigned to specific locations. No information technology resource shall be removed from County premises without express permission of the Department Head and MIS – this shall only be allowed for the purposes of completing County business.

E. **DUTY NOT TO WASTE OR DAMAGE COMPUTER RESOURCES.**

1. **Accessing the Internet**. To ensure security and avoid the spread of viruses, Users accessing the Internet through a computer attached to Jefferson County's network must do so through an approved Internet firewall or other security device. Bypassing Jefferson County's computer network security by accessing the Internet directly by modem or other means is strictly prohibited unless the computer is not connected to Jefferson County's network.
   a. User access may include Webcasts, Webinars, and other forms of on-line training for County business or practices that may include downloadable presentation or handouts. Connection should be made through an acceptable portal. Refer any questions or problems to MIS within a reasonable amount of time prior to start to allow trouble-shooting.
   b. Monitoring of Internet access is done periodically to collect statistics on use. There is a "history", including "cookies" stored internally on the computer to identify websites. MIS will determine if and when the monitoring or history require action such as deletion to increase the efficiency of the network.
2. **Frivolous Use.** Computer and telephone resources are not unlimited. Network bandwidth and storage capacity have finite limits, and all Users connected to the network have a responsibility to conserve these resources. As such, the User must not deliberately perform acts that

waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, staying on line when the browser is not in use for more than thirty minutes, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files, connection of an iPod, MP3 or other device, or otherwise creating unnecessary loads on network traffic associated with non-County-related uses of the Internet.

3. **Virus detection**. Files obtained from sources outside Jefferson County, including disks brought from home, files downloaded from the Internet, newsgroups, bulletin boards, or other online services; files attached to email, and files provided by customers or vendors, may contain dangerous computer viruses that may damage Jefferson County's computer network. Users should never download files from the Internet, accept email attachments from outsiders, or use disks from non-Jefferson County sources, without first scanning the material with Jefferson County-approved virus checking software. If an employee or other authorized User suspects that a virus has been introduced into Jefferson County's network, notify MIS immediately. All devices connected to the network must have virus protection installed on them by MIS and be updated at least bi-weekly or as otherwise directed by MIS.
4. **County Purchased Equipment.** All equipment connected to the Jefferson County systems and network must be authorized by MIS. Any violations of this will result in immediate disconnection from the Jefferson County system or network. MIS will consider requests for non-County equipment to be hooked-up to the Jefferson County network. MIS will examine each request and approve or deny the request. All equipment purchased is property of Jefferson County and is not the property of individual departments or individual Users unless the equipment is purchased through grant funds. If the equipment is purchased through grant funds, the grant terms determine ownership. This equipment must still conform to all of the standards maintained for County equipment. Loaner equipment is under the charge of MIS and shall be returned when the original piece of equipment is repaired or replaced. Personal hardware, software, and telephone items may not be connected to Jefferson County equipment.
    a. Only MIS staff may remove from inventory any information technology resource and either supervise the destruction of it or utilize a County-contracted facility for secure disposal or recycling following industry-accepted procedures.
    b. Under no circumstances shall a User take apart any information technology resource for any reason. Contact MIS for assistance in the event of equipment failure.
    c. County-owned printers and facsimile (FAX) machines (connected to the network) should be located in a secure area, away from unauthorized access. Any information printed must be considered and used as confidential as information viewed on the screen, to be stored or disposed of in a secure manner (for example, shredding) per the “Jefferson County Record Retention Schedule”.
5. **Security.** Computer security has grown into a compendium of laws, standards, and best practices designed to promote the protection of the computer and its network from internal and external attack, as well as the misuse of its contents by owners and protectors alike. Employees

and other authorized Users are reminded of their role in maintaining security.

a. Jefferson County employees and other authorized Users will be responsible for maintaining the confidentiality of their User IDs and passwords. Password selection and upkeep should follow guidelines received from MIS. When a User leaves their work area, the workstation or notebook should always be logged off completely following MIS protocol. **Employers and other authorized Users shall notify MIS immediately if they believe that a "Security Breach" has occurred. An example would be an "unauthorized user" who obtains an active User ID or password to gain access to the Jefferson County network or other Jefferson County secure resource.** It is the responsibility of the Department Head or MIS contact to notify MIS to revoke a User's access in the event of termination, re-assignment of duties or transfer within the County.

b. Biometrics, using personal measurements such as fingerprints, hand outlines, scanners, voice recognition, handwriting analysis and keyboard analysis to increase network access control, will be assessed by MIS for feasibility as the technology improves and becomes more cost-effective. Many of the same User responsibilities will apply as do now to User ID and password safeguards.

c. Different types of media vary in how easy they are to tap into, from wireless/radio with an antenna being the easiest to the hardest being fiber optic cable. Simple, land-based cordless telephones can be intercepted very easily; cellular telephones vary in complexity and susceptibility to unauthorized reception. Wireless transmission through any portable computer or device is less secure than a cable-connected terminal. Employees and other authorized Users are cautioned to be aware when transacting County business the level of security found at the location, the connection through which the information will flow, and the need for documentation as official County business.

d. The use of non-County equipment such as a cordless telephone or police scanner that may interfere with County-owned communication devices may need to be restricted, and therefore require approval by MIS.

e. Computers have been set aside for use by the general public, County nursing home residents and jail inmates. Any attempt by these parties to use other equipment should be reported to MIS for a re-assessment of need.

f. In situations when a contracted agent or consultant cannot be authorized as a User by MIS, an assessment of options shall incorporate the necessity of maintaining the security and integrity of the County network in the most cost-effective manner while accommodating the request. MIS will represent the County's interests when developing a feasible plan.

F. NO EXPECTATION OF PRIVACY. Employees and other authorized Users are given computers, Internet access, and telephones to assist in the performance of their jobs. Users should have no expectation of privacy in anything they create, store, send or receive using Jefferson County computer and telephone equipment, including personal communications.

The computer network and the information in it are the property of Jefferson County. Passwords in the computer or telephone systems do not imply privacy.

1. **Waiver of privacy rights.** Users expressly waive any right of privacy in anything they create, store, send or receive using Jefferson County's computer equipment or telephone or Internet access. Each User consents to allow authorized Jefferson County personnel access to and review of all materials created, stored, sent or received by User through any Jefferson County network device, telephone or Internet connection.
2. **Monitoring of computer and Internet usage.** Jefferson County has the right to and does monitor and log any and all aspects of its Computer system and telephone system including, but not limited to, monitoring Internet sites visited by Users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by Users. Department Heads and or MIS contacts and or MIS staff or contracted agents have access to User IDs and passwords and can use them at any time for monitoring purposes or allowing access during User absence or termination. Employees and other authorized Users should be aware of the text referring to monitoring on the computer screen at network sign-on.

   MIS will send advance notification to Users to schedule viewing and update sessions for which the User has not initiated the need for this interface.

3. **Blocking sites with inappropriate content.** Jefferson County has the right to and does utilize software that makes it possible to identify and block access to Internet sites containing sexually explicit or other material deemed inappropriate in the workplace.

   If you are trying to access a county business related website and it is blocked, please contact MIS. MIS will unblock that site for county business-related purposes. If this is out-of-normal business hours, and is necessary for you to do your job, call 920-723-3040 and you can reach MIS for assistance.

G. OTHER INFORMATION.

1. **Personal use of telephones.** An employee or other authorized User may use County telephones (including cellular telephones) to place or receive necessary personal telephone calls. **All local and long distance calls on either a County-owned land-based or cellular telephone do result in charges being assessed to the County and therefore all employees and other authorized Users must review their County telephone bill and make reimbursement to the County for personal calls.**
   a. Personal use of telephones, including personal calls received by a User, shall be kept at a minimum and restricted to rest periods and lunch periods, whenever possible. Employees may use a personally-owned cellular telephone to prevent charges on County-owned equipment, but must follow the same guidelines for appropriate use. An employee or other authorized User who makes excessive use of the telephone for placed and/or received personal calls during working time and in working areas may be subject to progressive discipline.

2. **Voice mail messages.** The County may access voice mail messages that are stored on County telephone systems, including cellular telephones, without obtaining the consent of the User. Employees and other authorized Users are discouraged from using voice mail for personal matters as it consumes hardware resources. When listening to voice mail messages, Users should be aware of the volume control and possibility of unauthorized users hearing the content.
3. **Contact Person.** Each Department has a contact for MIS issues. This person, (either the Department Head or another designated individual or individuals), acts as the prime contact for MIS issues. When individual Users have problems or questions, they should first seek out the Department contact as their first line of support. If the Department contact person does not know the answer, then the Department contact person will seek out MIS assistance. Any additional technical support, for instance from a vendor or other computer system such as State of Wisconsin, should be setup post-MIS contact.
4. **Vendors.** No vendors or outside entity shall come on site and be left alone with Jefferson County network access or related equipment without consent from MIS. When vendors come on site, they are required to make appointments with MIS at least 72 hours ahead of the visit. No vendor or outside entity shall be given any supervisory or administrative user names or passwords. (Resolutions 2001-17 and 2003-51).
    a. To be included in the term "outside entity" is auditors, management consultants and surveyors on County business.
    b. A non-network internet connection is recommended when a vendor or outside entity requests access for purposes of a training, meeting or demonstration. An alternate location or method for vendor use should be requested from MIS. A secured, on-line meeting is preferred for outside on-line vendor contact.
    c. If health care information is to be accessed, MIS will notify the County HIPAA Officer regarding the need for a signed Confidentiality Acknowledgment or HIPAA Business Associates Agreement.

H. COMPLIANCE WITH HIPAA AND OTHER REGULATIONS. The County faces increased regulatory pressure to protect the privacy of information collected on its citizens; ensure the accuracy of financial data; and audit and log efforts to comply with laws and regulations. Among these are the Sarbanes-Oxley Act (adherence to standards in financial record keeping), the Gramm-Leach-Bliley Act (protection of personal financial data), the U.S. Patriot Act (antiterrorism and law enforcement), the Health Insurance Portability and Accountability Act (secure transmission and storage of health care records), the Federal Trade Commission's Fair and Accurate Credit Transactions (FACT) Act of 2003 "Red Flags Identity Theft Prevention", and the amendments to the Federal Rules of Civil Procedure (e-Discovery). The later three are addressed here:

1. **Health Insurance Portability and Accountability Act of 1996 (HIPAA).** HIPAA is the comprehensive federal law covering the transactions and code sets used for the billing of health care services; and the privacy and security of protected healthcare information, within the covered entity departments of Jefferson County. HIPAA has been further enhanced by the American Recovery and Reinvestment Act of 2009, expanding its reach to covered entity contracted business associates, increasing enforcement rules and penalties, and adding the

Federal Trade Commission as a regulator of vendors of electronic health records and other electronic services. The HIPAA Officer is appointed by County Board Resolution to establish and maintain the documentation to fulfill requirements of this Act. The Privacy Rule covers an individual's right to control the acquisition, use, and disclosure of individually identifiable health care information. The Security Rule establishes the use of Administrative, Physical and Technical Safeguards to maintain the Confidentiality, Integrity and Accessibility of electronic protected health care information (ePHI). Both rules have patient complaint and mitigation of breach provisions. Prevention and detection of healthcare fraud is another focus of the Act. Outside contractors and consultants are required to sign a "Business Associate Agreement" listing the uses and disclosures of health care information. Employees and other authorized Users of health care information in the County's covered entity departments receive additional training on the HIPAA requirements. Areas that show the intersection of health care system needs and electronic security (for example, requests for wireless access) must be reviewed and approved by the Jefferson County HIPAA Officer.

a. Employees and other authorized Users may have access to the electronic care databases that replace paper medical records in the County's health care areas. These "Electronic Healthcare Records (EHRs)", clinical and billing, are covered by both the HIPAA Privacy and Security Rules. When purchased through MIS as a vendor software package, the vendor must sign a Business Associates Agreement detailing the HIPAA requirements. Software developed by MIS must likewise be compliant. Users must maintain proper security and privacy protections as outlined in this Ordinance and received through specific application training.

b. **Patient Request to Maintain a Personal Health Records (PHR)**. A request may be received to connect, download, or use on County property a computer, scanner, copy machine or other computer related equipment not owned by the County to assist a patient in maintaining their PHR. Review of these requests will be done on a case-by-case basis, with input from the health care department, HIPAA Officer and MIS.

c. **Nationwide Health Information Network**. NHIN is being developed to provide a secure, nationwide, interoperable health information infrastructure that will connect providers, consumers, and others involved in supporting health and healthcare. This critical part of the national health IT agenda will enable health information to follow the consumer, be available for clinical decision making, and support appropriate use of healthcare information beyond direct patient care so as to improve health. When the time comes, MIS will have a role in connecting the electronic health care databases within the County network to the national gateway.

2. **Federal Trade Commission Fair and Accurate Credit Transaction Act (FACTA) of 2003,** also known as "Identity Theft Prevention Program, Red Flags Policy". Identity theft, including the subset of medical identity, is addressed in a separate county policy covering the FACTA recommendations; the need for notification in the "Notice of Unauthorized Acquisition of Personal Information" per Wisconsin State Statute; and the best practice recommendations accumulated through the experience of consumers and providers who have dealt

with identity theft. Employees and other authorized Users should report to MIS any of these indicators of possible precursors to identity theft such as:

a. **PHISHING** - using enticing email masquerading as legitimate communications to bait the consumer into revealing sensitive information, frequently mimicking a bank to verify account information,

b. **DISHING -** using social engineering and voice communications to gain access to private personal and financial information over the telephone with false caller I.D. that mimics a legitimate company, and;

c. **SECURITY BREACHES -** involving the inadvertent disclosure or theft of personal information, which often are a means to acquire the information of another person for use in committing identity theft.

3. **Federal Rules of Civil Procedure, Amendments Effective December 1, 2006**. Commonly referred to as "e-Discovery", these are the amendments established by the United States Supreme Court and approved by the U.S. Congress to address the unique aspects of the electronic data discovery procedure for all civil suits in U.S. district courts. Also known as metadata (literally defined as "data about data"), this electronic background data has different meanings, depending on context. In the context of word processing documents, metadata is information that may be hidden from view on the computer screen and on a paper copy, but, when displayed, may reveal important information about the document. Legal commentary and federal cases addressing the treatment of metadata during litigation and civil discovery will also be helpful for understanding access and retention issues related to metadata. The influence of the rules is filtering down from the federal level into other legal areas.

a. Knowing what information is present within the County information technology system, its purpose within the County's role of public service, where it flows, and where it is stored is foundational to its protection and availability for e-Discovery. Users must be aware of the electronic data retention plan in the "Jefferson County Record Retention Schedule" to maintain data critical to County business in a retrievable format. Where not necessitated by valid business need, a strong effort should be made to minimize the retention and replication of data.

b. MIS is key to the County's response to such a request, and will initiate the specialized policies and procedures required to comply. In the event of receipt of an e-Discovery request, MIS will need full cooperation from any User accessing a computer system with electronic information covered by the e-Discovery request.

c. Employees and other authorized Users should be aware that home-based, personally-owned computers and portable devices cleared for work-related use outside of County offices may be discoverable under the e-Discovery process (even non-work related emailing between a home and a County-owned computer may raise the question that work was continued at home, opening up a personally-owned computer to the possibility of e-Discovery).

I. WIRELESS AND OFF-SITE USE CAUTION; TELEWORKERS.

Non-cable technology is used in wireless applications and in conjunction with other networks, such as a gateway between two Local Area Networks (LANs) separated by some geographical distance (e.g., across a body of water or a city). Microwave, radio and satellite is less secure than fiber, coaxial, and twisted pair cable because communications can be intercepted through the air via an antenna. The only way to increase wireless security is to encode the transmissions, which adds to the complexity of the communication process. Wireless connections within County facilities have been established by MIS only after a thorough assessment of the need vs. the risk of interception.

Users are reminded that other wireless setups are outside the supervision of MIS. Access to Jefferson County applications and databases on public internet connections should be done only after the User conducts a risk assessment for that particular location, including ownership of the computer equipment and the level of confidentiality for the information. Locations such as home, kiosk, hotel, state office, another county, library, airport, coffee shop or other public workstation or other Wireless Access Points (WAPs) constitute increased security threat. Risk assessment must include awareness of who else may be able to see the screen at time of entering a User ID and password and accessing the information; secure printing with destruction by shredding of copies to be disposed of; deletion of downloaded information from the computer prior to sign-off; and secure removal of any portable device. Because of the increased risk and possibility of such off-site use being denied, it is important to check the access policy for any state-developed or proprietary (software legally the property of another party) database. Do not connect to the Internet off-site for a designated, work-related purpose unless approval has been received from MIS.

Other cautions and recommendations follow:

1. **Social Engineering**. Teleworkers should be aware of how to handle threats involving social engineering, which is a general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious. For example an attacker might approach a teleworker in a coffee shop and ask to use the computer for a minute or offer to help the teleworker with using the computer. Teleworkers should be wary of any requests they receive **that could lead to a security breach or the theft of a telework device.**

2. **Social Networking**. Found in many forms, social networking focuses on building online communities of people who share interests and activities, or who are interested in exploring the interests and activities of others. Examples are: (Social Utilities e.g. Facebook, LinkedIn, MySpace, Twine, Twitter); Blogs (Web logs) - Web site usually maintained by an individual with regular entries of commentary, descriptions of events, graphics; Electronic Bulletin Board – password protected site for exchanging messages; Instant Messaging (IM) - form of real-time communication between two or more people based on typed text (e.g. AOL Instant Messenger); Music-sharing/File Sharing; P2P – Peer-to-Peer network that is a direct conduit between computers; Photo-sharing (e.g. Flickr and Zooomr) ; Personal Profiles; Really Simple Syndication (RSS) - an XML format designed for sharing Web content like news headlines; Social Bookmarking - a method for Internet Users to store, organize, search, and manage bookmarks of web pages on the Internet (e.g. del.icio.us and StumbleUpon); Virtual Worlds - a computer-based simulated environment intended for its

Users to inhabit and interact via textual, two-dimensional, or three-dimensional graphical representations; Whiteboards - the placement of shared files on an on-screen "shared notebook", allowing the User to mark up the electronic whiteboard much as one would with a traditional wall-mounted board; Wikis - page or collection of Web pages designed to enable anyone who accesses it to contribute or modify content, often used to create collaborative websites and to power community websites (e.g. Wikipedia.org); YouTube - a video sharing website where users can upload, view and share video clips; and other sites with functions similar to those listed. Users are strongly advised to research the social networking site's "Privacy Policy" for the: data retention schedule (how long and where, e.g. U.S. located servers, backup tapes); restrictions prior to using "cut and paste" and "copy and paste" functions; compliance with applicable laws; and the disclosure policy in response to lawful requests such as court orders and subpoenas. In the expectation of the continued interest in social networking, to increase awareness of potential risks, and to emphasize that there should be no expectation of privacy, Users must be aware of the following:

a. Unfortunately, there have been instances of computer breaches when a social networking participant inadvertently opens the computer and network to outside influence to virus/worm attack and unintentional sharing of confidential files with downloading or uploading of files. To minimize this risk, social networking is not allowed on work time except for an approved use in the employee's department. Even with approved use, employees and other authorized Users are to use caution when accessing any of the above-listed social networking sites from a work computer, including equipment authorized for use outside of County-owned buildings.

b. Lines may become blurred as to when personal information is overlapping with other areas of life, including what is happening in a User's work world. While interactions may seem limited to a restricted "circle of friends", the reality is that postings are very "public" and may be damaging to the user personally and professionally. Users of social networking sites have options within the framework of the site's "Privacy Policy" which may not fully protect the information posted as well as the User may think it will. Prior to deletion, information may have been printed and/or stored by a viewer. Even after deletion, information may remain on back-up tapes.

c. Inappropriate postings of work experiences may prove detrimental to the person posting and to co-workers, especially if it includes references by name. Before discussing County-related activities on any social networking website or while using any information technology resource, Users should consider the following: How does this posting reflect on you as a County employee? Your co-workers? Your work unit? The County? Are you including information that could directly (e.g., name, Social Security Number, address, etc.) or indirectly (e.g., provider name, date of birth, diagnosis, etc.) identify a patient under your care or the care of a County department? Is this confidential information that may constitute a breach under

County ordinance, and/or Federal or Wisconsin State Law or regulation? The following particular areas must be stressed:

1). Direct service providers in HIPAA-covered healthcare areas are cautioned about communicating as "friends" within social networking groups regarding County-related or healthcare business, either on County or personally-owned information technology equipment. The potential for a HIPAA-defined breach, with its attendant breach notification expenses and HIPAA-mandated fines, is too great a risk and cost. Instead, utilize other, secure methods of communication between you as a provider and the patient. Equally, employees and other authorized Users in all areas must be aware of any special requirements or best practices that cover the performance and documenting of their work duties prior to engaging in social networking conversations.

2). Posting of confidential, County information is prohibited and shall be considered a breach. Users may never access, discuss or use any County confidential information for personal, non-work related reasons. Information technology resources shall never be used to violate County policies on harassment, discrimination or for any illegal activities. Non-County sanctioned pictures, videos or live camera connections shall not be taken with either personal or County-owned equipment, and only with additional approval may County-sanctioned media be posted.

3). As already indicated in this "Computer, Internet and Telephone Use Policy/Ordinance", employees and other authorized Users should not have an expectation of privacy. You may be monitored at anytime by authorized county employees to maintain compliance with this Policy/Ordinance and for network security, which may incidentally expose private information that you may prefer not to share. In addition to general monitoring and receipt of a report of an alleged misuse, indication of your position with the County or other identifying information may open up your social networking use to searching by that descriptor.

Investigation and enforcement of the social networking policy shall extend to non-work related time. Users who become aware of postings of confidential County information are to report it with any evidence collected, even if subsequently "deleted", to their immediate supervisor for further action immediately. Corrective action per established protocol shall include removal of damaging information to the extent possible if not already undertaken, and notification of the individuals affected by the breach as required by law and best practice. Disciplinary measures, including reporting to higher authority for possible civil and criminal penalties, shall depend on the type and severity of the breach or misuse.

3. **Personal Firewalls on Teleworker Resources**. A personal firewall is a software program that monitors communications between a PC and other computers and that blocks communications that are unwanted. When properly configured, a personal firewall limits the ability of other computers to initiate communications with the telework PC. This can significantly reduce the exposure of the PC to network-based attacks, such as worms and protect shared resources on a PC. Teleworkers should read their personal firewall documentation carefully to gain a solid understanding of how it should be configured. If it is not clear how to do, **the teleworker should consult with MIS staff on configuring their personal equipment firewalls**. A personal firewall should be installed and enabled on every telework PC.
4. **Wired Home Networks**. Teleworkers should secure their wired home networks to help protect their telework devices. The most important part of securing most wired home networks is separating the home network from the network's Internet Service Provider (ISP) as much as possible. If a telework device connects directly to the teleworker's ISP, such as plugging the device directly into a cable modem, then the device becomes directly accessible from the Internet and is at very high risk of being attacked. Home network configurations are relatively complex to set up and maintain, so only Users who are proficient in networking and security should consider implementing configurations on their own; any teleworker unclear of how to setup **should consult with MIS staff on configuring their wired home network**.
5. **External Networks**. Teleworkers should be aware that networks other than their home networks are unlikely to provide much protection for their telework devices and communications, such as a laptop using a wireless hotspot at a coffee shop. Telework devices on external networks are also often directly accessible from the Internet. Because there is usually no easy way for teleworkers to determine what protection an external network might be providing for their devices, teleworkers should assume that third-party networks are **not** providing any protection and are at higher risk of being compromised. When teleworkers use a third-party network to access the County's computing resources, they should use a Virtual Private Network (VPN) or other secure remote access solution and should activate the secure remote access solution immediately after connecting to the third-party network. **If it is not clear how to set up a VPN or other secure remote access solution, the teleworker should consult with MIS staff**.
6. **Use of a WPA2**, **WPA**, **WPT** or **WEP key to protect access**. Depending on the options available, the Wi-Fi Protected Access (WPA2/WPA), Western Personnel Test (WPT), Wired Equivalent Privacy (WEP) key is a series of characters (either a password composed of letters, digits, and punctuation, or a hexadecimal number) that is used to limit access to a wireless network. A wireless Access Point (AP) can be configured to require each device to provide the same key as the one stored in the AP. Devices that do not know the key cannot use the wireless network. The key should be long and complex, making it difficult for others to guess. This should help to prevent people near the AP from gaining unauthorized access to the network. Best practices suggest strong encryption to protect communication using a key, to permit access for particular devices, changing the public name of a wireless network, setting the Service Set IDentifier (SSID) which essentially is a name that identifies a wireless network and

disabling wireless access for administration. **Teleworkers should consult with MIS regarding these technical requirements.**

Approved by Human Resources Committee, January 19, 2010.

Jefferson County

COMPUTER, INTERNET AND TELEPHONE USE POLICY ACKNOWLEDGMENT of UNDERSTANDING

Access on a need to know and minimum necessary basis is granted to Jefferson County equipment, software, network, Internet and telephone systems by employees or other authorized users. It is expected that all users have a responsibility to utilize the Jefferson County computer resources, Internet and the telephone in a professional, lawful and ethical manner. Those not directly assigned use are expected to acknowledge with signature the same policy as those who are. There should be no expectation of privacy in anything that is created, stored, sent or received using Jefferson County computer and telephone equipment. Use of county computer resources may be monitored. Only equipment and software approved by MIS may be installed. Any reimbursable costs incurred for personal use of Jefferson County resources, equipment or telephones must be paid. Users are expected to maintain the confidentiality of assigned User I.D.'s and passwords, and to secure assigned equipment and workstations.

The Computer, Internet and Telephone Use Policy will be as amended from time-to-time, but is the policy as of the day signed. Look to the Personnel Policy for Employees of Jefferson County for the latest version of the Policy at: https://www.co.jefferson.wi.us/jc/employee/index.php, or as available in print copy as posted within departments, and upon request for those without computer access.

Individual county departmental policies and procedures to further reinforce the understanding of information technology use will be reviewed during orientation and training, including the standards of the Health Insurance and Portability Accountability Act (HIPAA) in regards to Protected Health Information (PHI) if it applies. Violation of any federal, state or county information technology policy may result in disciplinary action, including possible termination and civil and criminal penalties, as further detailed in HIPAA or other information technology specific rules.

By my signature below, I acknowledge that I have read, understand and agree to comply with the terms of Policy governing the use of Jefferson County computer, Internet, network, telephone and other related equipment. I understand that loss of privileges, sanctions or other actions up to and including termination may be imposed for failure to follow the Jefferson County Computer, Internet and Telephone Use Policy.

_____ _____

Signature of Employee/Volunteer/Other Designated **Date**

_____

Printed Name

02/2010

To be filed in Human Resources/Volunteer/or Other Designated File