



# Board of County Commissioners Agenda Request

## 20

Agenda Item #

**Requested Meeting Date:** 11 February 2025

**Title of Item:** MCIS Hosting agreement

<input type="checkbox"/> REGULAR AGENDA <input checked="" type="checkbox"/> CONSENT AGENDA <input type="checkbox"/> INFORMATION ONLY	<b>Action Requested:</b> <input checked="" type="checkbox"/> Approve/Deny Motion <input type="checkbox"/> Adopt Resolution (attach draft)	<input type="checkbox"/> Direction Requested <input type="checkbox"/> Discussion Item <input type="checkbox"/> Hold Public Hearing* <small>*provide copy of hearing notice that was published</small>
<b>Submitted by:</b> Chris Sutch		<b>Department:</b> I.T.
<b>Presenter (Name and Title):</b> Chris Sutch, IT Manager		<b>Estimated Time Needed:</b> 0
<b>Summary of Issue:</b>  <p>MCIS has requested a contract change due to a change in hosting circumstances. Previously Aitkin County's IBM-i server was hosted by MCIS in Itasca County's data center. Due to changing requirements, this was moved to the Paul Bunyan Communications data center in Bemidji MN.</p> <p>Jim Ratz, Aitkin County Attorney has reviewed the referenced contract with revisions and finds it to be appropriate as to form and content.</p>		
<b>Alternatives, Options, Effects on Others/Comments:</b>  		
<b>Recommended Action/Motion:</b> Approve and sign attached contract.		
<b>Financial Impact:</b> <i>Is there a cost associated with this request?</i> <input type="checkbox"/> Yes <input checked="" type="checkbox"/> No <i>What is the total cost, with tax and shipping? \$</i> <i>Is this budgeted?</i> <input type="checkbox"/> Yes <input type="checkbox"/> No <i>Please Explain:</i>		

Legally binding agreements must have County Attorney approval prior to submission.



**Minnesota Counties Information Systems**

413 SE 7th Avenue, Grand Rapids, MN 55744

Phone 218-326-0381

**MINNESOTA COUNTIES INFORMATION SYSTEMS  
HOSTING AGREEMENT**

This Hosting Agreement is made by and between **Minnesota Counties Information Systems (MCIS)**, a Minnesota joint powers entity, and **Aitkin County**, a Minnesota political subdivision (Hosted Entity).

1. Hosted Entity (f/k/a County, Member) is a member of the MCIS joint powers entity, as defined by the MCIS Joint Powers Agreement.
2. Hosted Entity owns and operates IBM-i (f/k/a iSeries, AS/400) server on which they run various software programs related to the Hosted Entity's statutory functions, or the Hosted Entity is a current subscriber to the MCIS hosted solution.
3. The ~~IBM-i~~ server, peripheral backup hardware, and operating system software require staff with sufficient expertise to operate, monitor and support.
4. Hosted entity finds it difficult for individual political subdivisions to maintain staff with expertise on the IBM-i server, peripheral hardware, and operating system, and/or it is not cost effective to maintain this expertise.
5. As a solution, MCIS offers a hosted environment whereby MCIS acquires and maintains the requisite IBM hardware in a suitable location and hosts the software and data needed by the political subdivisions.
6. This Hosting Agreement sets forth the terms and conditions of the hosting relationship between MCIS and the Hosted Entity.

**Definitions**

1. Budget Year. January 1<sup>st</sup> through December 31<sup>st</sup> with the budget for the new year approved at the MCIS Board meeting in July of the current year.
2. Planned Date. The month/year, provided upon signing, a hosted entity desires to be implemented.
3. Implementation or Calculation Date. The month/year both parties agree to target for implementation.
4. Co-location equipment. Equipment, which is composed of physical hardware and software to operate equipment, located at co-location facility which could include but not limited to IBM-i server, Cybernetics device (disk to disk backup), router/firewall, switches (layer 2 or above), power distribution unit (PDU), IBM tape drive(s), IBM hardware management console (HMC), uninterruptible power supply (UPS). Asset listing can be provided upon request.
5. Wide Area Network (WAN). Technology that spans beyond a single facility to connect multiple locations together, such as MCIS offices, co-location facility, members facility, cloud applications and/or storage. MCIS signed a contract running through 2029 with Paul Bunyan Communication to provide internet connection into the co-location facility, and metro-ethernet connections between MCIS offices and Paul Bunyan, and Itasca County and Paul Bunyan. All other member counties are connected via virtual private site to site connections (i.e. VPN).
6. Co-Location facility (Co-Loc). Physical location housing the WAN and co-location equipment. In addition to the WAN and cabinet space for the co-location facility, it provides 24-hour security monitoring, fire suppression, and redundant power, cooling and broadband connectivity.
7. Replacement Year. Year the hardware for the hosted environment is planned for upgrade, which is currently defined to July/August of 2028 for Cybernetics Equipment and July/August 2029 for IBM-i equipment. MCIS maintains the right to revise dates based on performance/capacity needs and with approval by the MCIS Board.
8. LPAR. A partition created on the shared IBM-i server for the hosted entity.
9. Device(s). Electronic data processing equipment which can be set up to access the LPAR, such as but not limited to servers, laptops, desktop, cell phones, printers, scanners, tape drives, and so forth.
10. MCIS Software - applications and utilities used for MCIS developed software such as Property Tax, CAMA, Payroll/HR, and MCISQGPL utilities.



11. MCIS 3<sup>rd</sup> Party utilities - Fresche Presto runtime; CNX Valence; ICS FormSprint runtime w/PDF and email, Kisco iEventMonitor and SafeNet/I, ProData Data Base Utility (DBU), and future solutions that may be approved by the MCIS Board.
12. MCIS Desktop utilities - IBM-i Access Client solutions, Start PC Command.
13. Non-MCIS software – all other software not defined as MCIS software, 3<sup>rd</sup> party and/or desktop utilities. Examples such as TriMin IFSpi, Social Welfare, Highway Costing, and so forth. MCIS will require a list of the software, vendor contact information, and the Hosted Entity product owners.
14. Hosting Data Storage – storage that cannot be removed and required to keep the system running, such as but not limited SSD, SCSI, NVMe drives related to hosting IBM-i server(s), Hardware Management Console, and Cybernetics equipment.
15. Managed Service Provider (MSP). Vendor providing configuration and on-going support for co-location non-IBM-i equipment, such as non-IBM-i server(s), switches, router/firewall, PDUs, extended endpoint detection and response, multi-factor authentication (MFA), Microsoft 365, WAN communication and so forth.
16. Removable media – portable devices that can be connected to computer hardware to provide data storage that can be removed while the system is running and not required to keep hardware operational, such as but not limited to USB memory stick, external hard drives, tapes, CDs, and DVDs.

### Terms

1. **Effective Date.** This Hosting Agreement is effective upon signing.
2. **Hosting Services**
  - a. MCIS will provide hosting servers and all necessary ancillary equipment, backup tapes, support, and maintenance to host the Hosted Entity's applications and data ("the Services"). MCIS will provide the processor capacity, disk space and memory to run the Hosted Entity's IBM-i applications. The specifications of the hardware used for hosted services shall be determined by MCIS at its sole discretion.
  - b. The co-location equipment will be placed at co-loc facility, which is determined by MCIS and approved by the MCIS Board. MCIS selected Paul Bunyan Communications' data center in Bemidji, MN as the co-Loc facility, and is under contract through August 2029. MCIS is responsible for maintaining/supporting IBM-i and Cybernetics hardware/software associated co-location equipment.
  - c. WAN communications are determined by MCIS and approved by the MCIS Board. MCIS selected Paul Bunyan Communications as the WAN provider and is under contract through August 2029.
  - d. MSP provides services to support specific co-location equipment and WAN service offerings, which is determined by MCIS and approved by the MCIS Board. The term of this contract is year-to-year, and the provider selected is Paul Bunyan Communications.
  - e. MCIS will perform daily backups to a disk-to-disk backup system with replication of the daily backups to MCIS offices. Monthly and yearly backup to physical tape. Maintaining fifteen-month rotation of monthly's and seven-year rotation of yearlies. The Hosted Entity reserves the right to specify a different retention schedule in writing. MCIS stores tapes in a safe rated for sixty minutes at 1,350 degrees.
  - f. The Hosted Entity reserves the right to specify a different retention schedule in writing, and MCIS obtains the right to determine additional charges if applicable.
  - g. The Hosted Entity is responsible for providing all equipment and/or software necessary at the Hosted Entity's place of business for the Hosted Entity to access the hosted environment provided by MCIS and for maintaining applicable software licensing.



### 3. Hosting Fees

- a. **Start-up Fees.** This fee is specific to entities not implemented on or before January 1, 2025. The fee will be a pro-rated costs of quarterly reserve and yearly fees based on the calculation date, and possible co-location equipment upgrades, software transfer fees, and connection setup fees charged by Co-Loc, WAN, and/or MSP providers. This fee will be invoiced at the beginning of the first quarter following the implementation date.
- b. **Reserve Fee.** Allows MCIS to build up funds for future upgrades to the co-location equipment, which includes vendor transfer fees, pre-paid maintenance over multiple years, and disaster recovery (DR) fee. The DR fee is a yearly cost charged to hosted entities to support upgrades to the IBM-i development server<sup>4</sup>, which is located at the MCIS offices and a pre-configured partition that the hosted entity's LPAR can be restored to in event of a declared disaster to the Hosted IBM-i server. The Hosted Entity is responsible for this fee as follows:
  - i. Hosted Entity having services on or before January 1, 2025, will be committed from January 2025 through replacement year.
  - ii. Hosted Entity implemented after January 1, 2025, will be committed from the calculation date through the replacement year.

The reserve fee will be invoiced as follows:

- i. Invoices are sent quarterly for the next three months of reserve fees due.
  - ii. If Reserve Fees available, in the replacement year of equipment upgrades, does not cover the expenses, then MCIS reserves the right to determine a fee for the next budget cycle to handle the uncovered expense with approval by the MCIS Board.
- c. **Yearly Fee.** The Hosted Entity shall pay a pro-rata share of the yearly maintenance, related supplies, WAN, Co-Loc, and security fee defined as follows:
    - i. **Yearly Maintenance.** Fee charged by vendors for yearly maintenance on co-location facility once the pre-paid maintenance expires. If the vendor allows, typically purchase three years prepaid (minimum) on critical equipment with 24 x 7 coverage. Otherwise, deal within the parameters of the vendor maintenance offerings.
    - ii. **Supplies.** Miscellaneous items budgeted for in support of hosted environment, such as LTO Tapes, cabling, and so forth.
    - iii. **Co-location Fee.** The hosted entities share a percentage of the total monthly fee with remainder applied to the MCIS general budget. Note all counties in some forms are connected into the co-location facility. The percent allocated to hosting is determined based on number of hosted entities in relation to total members.
    - iv. **WAN Fee.** Hosted entities will pay a percentage of the total co-location facility provider WAN fee with remainder applied to MCIS general budget. MCIS development/support environment is estimated to use the majority of the WAN communication setup (i.e. 60%).
    - v. **Security Fee.** Hosted entities share of subscription and/or maintenance fees for potential security solutions such as but not limited to Kisco SafeNet/I, MFA, and/or database encryption tools that may be required in the future with MCIS Board approval.
    - vi. Hosted entities are responsible for their portion of the co-location and WAN fees through August 2029. The supplies and hardware/software maintenance fees will be year-to-year.

The fee is determined as part of the MCIS annual budget approval process, and invoiced as follows:

- i. If the Hosted Entity was implemented prior to January 1, 2024, then fees for the budget year are invoiced quarterly.
- ii. If the Hosted Entity was implemented after January 1, 2024, then fees will be invoiced starting the quarter following the implementation date and quarterly thereafter.





## Minnesota Counties Information Systems

413 SE 7th Avenue, Grand Rapids, MN 55744

Phone 218-326-0381

- d. Reserve and Yearly fees can be revised during the yearly budgeting process with approval by the MCIS Board. This ensures yearly expenses are properly covered and reserve fees are being accumulated to handle the upgrades of co-location equipment.
- e. Service Fee. The Hosted Entity will determine the “level of service” they want provided by MCIS during the yearly budgeting process (reference Exhibit 1 for Definitions of Levels of Service), and each level’s monthly fee is set by the MCIS Board during the annual budget process. A Hosted Entity can move up a service level but cannot move to a lower service level once the MCIS Budget is approved. Fee is payable as follows:
  - i. All fees are based on the calculation date.
  - ii. The first invoice occurs the first quarter after the implementation date and includes the number of months from the calculation date through the ending month of the last quarter MCIS has invoiced for multiplied by the selected level monthly service fee.
  - iii. Thereafter, on a quarterly basis, the hosted entity will be invoiced for the next three months multiplied by the selected level monthly service fee.
- f. If amounts owed by the Hosted Entity become past due, the Hosted Entity is subject to the penalties and restrictions set forth in the MCIS Joint Powers Agreement and/or Bylaws.

#### 4. Security Requirements

It is of paramount importance that the Hosted Entity’s LPAR is secure. The Hosted Entity is responsible for maintaining security controls to prevent breaches from occurring on their network and infiltrating the LPAR. Security controls such as but not limited to are as follows:

- a. MCIS developed software requires a County to:
  - i. Maintain the current release level defined for MCIS’s software, 3<sup>rd</sup> Party, and desktop utilities.
  - ii. For MCIS desktop utilities County IT will distribute/update on the required county personnel devices within a reasonable time-period required by MCIS.
  - iii. Comply with “IBM’s Level 30 or 40 security controls” as described in Exhibit 2 (Defining MCIS Security Level 30/40)
  - iv. Anti-virus and/or end point detection recovery (EDR/XDR) tools on devices accessing the LPAR.
- b. Properly manage IBM-i user profile:
  - i. Ensure county personnel secure their IBM-i user profile passwords to guard against and prevent unauthorized access.
  - ii. Restrict sharing of IBM-i user profiles, except in the instance of IBM system profiles, MCIS operations profile, and/or what’s agreed to between the Hosted Entity and MCIS.
  - iii. Implement add, change, and enabling/disabling procedures with County staff.
  - iv. Implement procedures for restricting access of terminated employees on a timely basis.
  - v. Implement procedures for review/approval when granting IBM-i’s advanced special authorities to user profiles.
- c. Alert MCIS to the following:
  - i. User profiles that need to be disabled due to termination, moving to another department where access is no longer needed.
  - ii. Immediately on a security incident/breach on and/or to Hosted Entity’s network that present risk to the IBM-i server.
  - iii. MCIS will alert Hosted Entity IT Director of security incident breach on MCIS network that present risk to the remote IBM-i server.
- d. When disposing of hosted data storage and/or removable media, MCIS will adhere to the *NIST Special Publication 800-88R (Exhibit 4)*. In the event the hardware doesn’t conform to this data sanitization standard, then MCIS will remove the hosted data storage components perform the purge techniques (crushing, degaussing, shredding) of the NIST standards. Any disposal costs occurred will be distributed evenly between the hosted counties on the next billing cycle.
- e. MCIS reserves the right to require the Hosted Entity to procure and maintain security software solutions that were agreed upon by the majority of the Hosted Entities and approved by the MCIS Board.



- f. MCIS reserves the right to maintain or not maintain Cyber Security Liability insurance as directed by the majority of hosted entities and/or MCIS Board.
- g. In the event of a security breach within the IBM-I hosting environment, guidance described in the Security Committee Charter will be followed (Exhibit 3).
- h. MCIS utilizes an automated alert messaging tool to receive timely notification of issues occurring on a counties IBM-i partition. It is required that a county allows these messages to be emailed from the county's partition to specific individuals who are part of the MCIS email domain mcis.cog.mn.us and mcismn.gov.

Notwithstanding any other term or agreement to the contrary, each Hosted Entity is solely liable for any and all data breaches that occur within their designated IBM-i partition and agrees to defend and indemnify MCIS and County renting hosting facility space, power and network connectivity from any claims arising from such data breaches.

**5. Term.**

- a. This Agreement commences on the Effective Date and extends through December 31 of the Replacement Year.
- b. Any party may terminate this Agreement without cause upon 180 days' written notice to the other parties. In addition, this Agreement may be terminated if a party provides written notice of a breach of this Agreement and the breaching party fails to cure the breach within 60 days after receipt of the notice. If the Hosted Entity is the breaching party, it remains responsible for the start-up and service fees for the remainder of the budget year. For yearly fees their allocation of the WAN and co-location fees, and allocation of Reserve fees through the replacement year.
- c. If the Hosted Entity terminates this Agreement without cause by April 1 of the current year, then the Hosted Entity is not responsible for the Service fees after December 31 of the current year. If a Hosted Entity terminates without cause after April 1, then the Hosted Entity remains responsible for the Service and Maintenance fees for the current and next budget year regardless of the date of termination. If the Hosted Entity terminates this Agreement without cause prior to the December 31<sup>st</sup> of replacement year, the Hosted Entity remains responsible for payment in full of their allocation of the Reserve, Co-location, and WAN fees through December 31<sup>st</sup> of the replacement year. The Hosted Entity acknowledges that the financial structure of the MCIS hosting service depends on guaranteed receipt of Reserve, WAN, and Co-Loc during the entire term of the hosted agreements. This clause shall survive termination of this Agreement.

**6. Indemnification and Limitation of Liability**

- a. To the extent allowed by law, MCIS and the Hosted Entity shall fully defend and indemnify and hold harmless the other party against all claims, losses, liability, suits, judgments, costs, and expenses by reason of action or inaction of the employees or agents of the indemnifying party arising in whole or in part from any act or omission of the indemnifying party, its subcontractors, and their agents, servants, or employees, incidental to the performance of this Agreement. This agreement to indemnify and hold harmless does not constitute a waiver by any party of limitations on liability under Minnesota Statutes Section 466.04 and other applicable law or rule.
- b. To the full extent permitted by law, actions by the Parties pursuant to this Agreement are intended to be and shall be construed as a "cooperative activity" and it is the intent of the Parties that they shall be deemed a "single governmental unit" for the purposes of liability, all as set forth in Minnesota Statutes Section 471.59 subdivision 1a(a); provided further that for the purposes of this statute, each party to this Agreement expressly declines responsibility for the acts or omissions of the other Party.
- c. The parties to this Agreement are not liable for the acts or omissions of the other Party to this Agreement except to the extent to which they have agreed in writing to be responsible for acts or omissions of the other Party.



**7. Representations and Warranties**

Each party represents and warrants that the execution and performance of this Agreement has been duly authorized and the signatory to this Agreement possesses all necessary authority to enter into the Agreement.

**8. Data Practices**

- a. All data created, collected, received, stored, used, or maintained on the MCIS equipment and on or through the associated Hosted Entity network equipment is subject to the requirements of the Minnesota Government Data Practices Act (MGDPA). All parties shall abide by the provisions of the MGDPA, the Health Insurance Portability and Accountability Act and implementing regulations, and all other applicable state and federal laws relating to data privacy.
- b. The parties hereto acknowledge that MCIS is only providing a hosting environment for the Hosted Entity's data. Data content is the sole responsibility of the Hosted Entity. All data requests under the MGDPA are to be responded to by the Hosted Entity as the responsible authority for the data. Any requests for data, or for changes, additions, or deletions to data, received by MCIS from a third party shall be forwarded to the Hosted Entity for response.
- c. The Hosted Entity shall annually provide MCIS with an authorization to access the data for the sole purpose of carrying out its hosting obligations under this Agreement.

**9. Relationship**

This Agreement does not create a partnership, joint venture, or other business combination between the parties. Each party is responsible for its own insurance.

**10. Force Majeure**

No party shall be in breach of this Agreement in the event they are unable to perform their obligations as a result of natural disaster, war, emergency conditions, labor strife, the substantial inoperability of the Internet, the substantial inoperability of the State's WAN, or other reasons beyond their reasonable control, provided, however, that if such reasons or conditions remain in effect for a period of more than 30 days, any party may terminate this Agreement without further liability to that party.

**11. Notice**

Any notices required or permitted to be given under this Agreement shall be written in letter/memo form on company letterhead, signed on behalf of the party providing notice, and deemed received (1) upon receipt if personally delivered, which includes email; (2) on third day after mailing if sent by certified mail, return receipt requested; or (3) the next business day if sent by messenger or reputable overnight courier. Notices shall be sent to the following addresses:

Current MCIS Executive Director  
Minnesota Counties Information Systems  
413 S.E. 7<sup>th</sup> Ave.  
Grand Rapids, MN 55744

Current MIS/IS Director/Manager  
Aitkin County  
307 2<sup>nd</sup> St NW  
Aitkin, MN 56431

**12. Assignment**

No party shall assign its rights or delegate its duties under this Agreement without receiving prior written consent of the other parties.



**Minnesota Counties Information Systems**  
 413 SE 7th Avenue, Grand Rapids, MN 55744  
 Phone 218-326-0381

**13. Waiver**

The waiver of any provision or the breach of any provision of this Agreement shall not be effective unless made in writing. Any waiver by either party of any provision or the breach of any provision of this Agreement shall not operate as, or be construed to be, a continuing waiver of the provision or the breach of the provision.

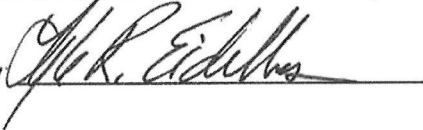
**14. Execution**

This Agreement may be executed in one or more counterparts, each of which shall be deemed an original and to constitute one and the same instrument. Electronic copies shall be considered originals.

**15. Miscellaneous**

This Agreement constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior and contemporaneous agreements, documents, and proposals. Any amendment or modification to this Agreement shall not be valid unless such amendment or modification is in writing, signed by authorized representatives, and references this Agreement. Any and all causes of action between any party arising out of or related to this Agreement shall be venued in Itasca County District Court.

**Minnesota Counties Information Systems**

By 

Lyle Eidelbes - MCIS Executive Director  
 Approval to sign provided on January 23, 2025, MCIS Board Meeting

Dated: 1/27/2025

**COUNTY OF AITKIN**

By: \_\_\_\_\_

\_\_\_\_\_  
 Print Name

Its: \_\_\_\_\_

Dated: \_\_\_\_\_



## **EXHIBIT 1 – LEVELS OF SERVICE**

### **Definitions**

- Please reference the main contract for other definitions that may be used with this exhibit.
- Hosted / On-Site Support – a Member County with an LPAR on MCIS provided equipment that is hosted at Itasca County defined datacenter(s)
- Remote Support – a Member County who desires their IBM-i server and/or LPAR manage by MCIS< but the physical server is at the County or location outside MCIS known data centers.
- MCIS Software - applications and utilities used for MCIS developed software such as Tax, CAMA, Payroll/HR, and MCISQGPL utilities.
- MCIS 3<sup>rd</sup> Party utilities - Fresche's Presto runtime; ICS's FormSprint runtime w/PDF and email, ProData Data Base Utility (DBU), and future solutions that may be approved by the MCIS Board.
- MCIS Desktop utilities - IBM-i Access Client solutions, Start PC Command.
- Non-MCIS software – all other software not defined as MCIS software, 3<sup>rd</sup> party and/or desktop utilities. Examples such as TriMin's IFSpi, Social Welfare, Highway Costing, StandGuard, iTera High Availability and so forth. MCIS will require a list of the software, vendor contact information, and the Hosted Entity product owners.
- Product Owner – County user(s) assigned as owner of a non-MCIS software, and/or County IT Director or County staff managing network security access.

### **Hosted On-Site County**

A member of MCIS Joint Powers who has a partition maintained and supported by MCIS on the IBM-i server(s) located at Itasca County. In 2024 MCIS is reducing support levels from three to two levels that members can select. Under the Level 2 support section ignore items that say "Remote Support" only. Support chosen is for the single LPAR assigned to the member on MCIS Hosted IBM-i server, and a preconfigured LPAR for disaster recovery on the MCIS Development IBM-i server.

### **Remote Support County**

A member of the MCIS Joint Powers who has their own IBM-i server at a designated county location and desires the server to be managed by MCIS staff remotely. This service is called Level 4, and duties performed of level 2, 3 and others will be identified in the section titled "Level 4 – Remote Support and/or County Specific Requests". Level 4 assumes management of one IBM-i server with one active partition, unless otherwise noted. This IBM-i server will be called "Production".



### **Level 2 – Basic Support and control MCIS Applications**

Focused on basic IBM-i operational duties and activities related to the MCIS Software. All on-site and remote hosted entities are required to take this level of support.

#### **Requirement of Hosted Entity (County) – On-Site and Remote Support**

- MCIS requires the County to designate an individual(s) that will coordinate IBM-i tasks that need to be physically performed at their location(s) such as but not limited to setup of user application on desktop/personal devices, printers.

#### **Backups – On-Site and Remote Support**

- Managing, monitoring, and configuring daily, weekly, monthly, yearly partition backups.
  - Review daily backup results to ensure successful completion.
  - Restore objects from previously available backups as needed.

#### **Backups – On-Site Support**

- Uses MCIS backup application included with the MCIS developed software.
- Scheduling of the standard “MCIS Full System Save” applications/process.
- Daily backups are retained on disk-to-disk backup technology called Cybernetics.
- Maintain a minimum of 35 daily tapes. The current procedure as of 2024 is to perform a 45-day rotation.
- Cybernetics technology for deduplicating and replicating virtual tapes is utilized.
- Daily the backups are sent to a secondary Cybernetics device for DR purposes. The secondary device stores only the current week of backups.
- Perform monthly backup to physical tape and maintain a 15-month rotation.
- Perform yearly backups to physical tape and retain up to 7 years.
- Physical tapes are stored in the safe at MCIS offices.
- Note - Tape technology changes with every upgrade cycle of IBM-I hardware that is scheduled every 5-6 years. Physical tape media that hasn't been cycled out and the new tape technology does not support may have to be sent to a 3<sup>rd</sup> party to duplicate the tape to the current technology. This will not be done until that specific tape is required. Most new tape technology can write's back one prior version but reads up to two versions back.

#### **Backups - Remote Support**

- MCIS will follow the standard established by the County using the hardware currently performing backups of the IBM-i server(s) at the County.
- Any standard that deviates from the hosted/on-site configuration may require training from County personnel and/or vendor, such as but not limited to operation use of software performing backups, current daily procedures, management of hardware storing backups, and so forth.
- MCIS recommends County utilize the hosted/on-site backup methodology, within reason, for easier operation by MCIS.

#### **Systems Operation – On-Site and Remote Support**

- Monitor/respond to issues with nightly jobs the morning of each business day, such as backups, system start-up tasks, and daily, weekly, monthly jobs scheduled to run at night.
- Manage adding, changing, disabling, and enabling of base IBM-i user profile.
- Provide consultation on connecting laptops/desktop/servers' applications to the member's IBM-i partition's databases/applications, such as Access Client Solution (ACS), ODBC, FTP, and so forth. But not responsible for deploying/configuring the connection on non-IBM-i devices.
- Assist with configuration and/or issues occurring on print devices directly configured to iBM-i.
- Monitoring subsystems, job queues, QSYSOPR message queue, PhP logs, Apache logs related to MCIS developed applications.





- Installing/managing i-EventMonitor software and coordinating responses to alerts provided.
- Applying PTF, OS upgrades to IBM-i operating systems as needed.
- Applying patch and release updates to MCIS developed software, and utilities used for MCIS development and operational support, such as but not limited to Fresche Presto product, ProData's DBU, and ICS FormSprint product.
- Setup scheduled nightly jobs required by MCIS Software, and/or those requested by County user(s).
- Perform MIS tasks associated with MCIS developed Tax/CAMA and Payroll.HR software checklists.
- Troubleshooting hardware/OS related issues and coordinating actions with IBM.
- Coordinate network issues resolution with member's IT Staff, facilities networking staff, and MCIS.

#### **DR Recovery Planning/Testing – On-Site Support**

- Maintain the disaster recovery and business continuity plan for the IBM-I environment.
- Perform the disaster recovery plan when required.
- Provide a pre-configured partition on the MCIS Development IBM-i server, that allows for faster DR recovery than starting from scratch.
- Perform testing on at least one member's partition per year. The goal is to cycle through members over a five to six-year period. Includes a connectivity test with member's IT staff.
- Note, recovery processes between partitions are similar, and all members can leverage the results of the yearly test as documentation for their auditors.

#### **DR Recovery Planning/Testing – Remote Support:**

- Assist as needed in disaster recovery and business continuity planning for the IBM-I environment.
- Assist with DR recovery test coordination when defined by the County.
- Assist with DR recovery of the IBM-i under the direction/coordination of the County

#### **Audit Reporting – On-Site and Remote Support**

- Configure IBM-i standard security auditing capabilities and specific audit controls the MCIS MIS User Group agrees to.
- Hosted entities can request additional controls to be audited and reported on.
- Schedule the monthly security audit reports, and alert member's security team of location and timing for availability.

#### **Configure and Administer General System Clean-up – On-Site and Remote Support**

- Configure MCIS standard process for aging output queues and files stored in user's primary integrated file folder (IFS), and so forth.
- Clean up of MCIS created folders for release installation, and standard MCIS and IBM journal receivers.
- Configure any override of folders County IT department specifies should have different days to retain or ignored all together.
- Monitor disk usage for spikes in abnormal usage and provide information to County IT of how to handle.

#### **On-boarding Coordination – On-Site and Remote Support**

- Review roles, responsibilities, and expectations with County that are currently handled by county staff as it relates to the IBM-i to establish the level of support.
- Coordinate the communication of how county's users will transition to the new support model.
- Perform assessment of current security configuration on its adherence to MCIS operations team minimal requirements and IBM Level 30/40 or above standards
  - Provide an assessment of what is needed to meet the standards.
  - Create a plan and target date with the member to meet standards.



- If needed, the county and MCIS will mutually agree to go live not meeting standards, but both will diligently and faithfully work to reach adherence on or before the established target date.

#### **Additional On-Board Coordination - On-Site Support**

- For hosted/on-site entities, build/execute the plan for: project startup for roles/responsibilities and timeframes; network setup/configuration; application software assessment for communication with non-MCIS vendors; assist with setup of Robocopy for CAMA images/sketches; partition configuration; testing the environment; and go live.

#### **Security Considerations/Handling – On-Site and Remote Support**

- The member must maintain IBM Level 30/40 security standards or above as outlined in Exhibit 2.
- Devices connecting to the IBM-I (user desktop, laptop, servers), and connecting within must have appropriate anti-virus and/or End Point Detection/Resolution software installed and ensure map drives to IBM-i are protected.
- Upon termination/departure of employee(s). County will notify MCIS through a help desk ticket to disable user profile within 24 hours of departure, assuming network profile was disabled immediately upon departure. In addition, the County will indicate timing for full removal of terminated employee user ID and owned objects.
- County ensures that 3<sup>rd</sup> party's supporting non-MCIS Software access is controlled by Product Owner. If a vendor is granted high level access (i.e. can go anywhere in the system) that County is responsible for monitoring access and managing the vendor according to the County's security policies, and MCIS security policy for on-site hosted counties.
- MCIS will manage basic security access to the IBM-i platform which will involve:
  - Establish procedures with County IT on how to handle non-MCIS vendor access to their partition.
  - Performing add, change, enabling/disabling of the IBM-i user profile.
  - Setup user access to MCIS developed software and required utilities used by MCIS software.
  - MCIS will utilize the MCIS menu solution to designate options they may need access to and/or direct them to the specific software they need access to.
  - Setup drive shares with required security settings specified for users, as needed.
  - Assist in configuration of security certificates on the IBM-i
- Yearly actions
  - MCIS will provide list of active users and last date of log in to the County IT Director
  - County IT Director will review and determine what action should be taken for disabling and/or removing the user(s).
  - MCIS will coordinate the activities for rename of objects owned with inactive/disabled profiles.

#### **Security Considerations/Handling – On-Site Support**

- Security fundamentals
  - At a minimum, non-MCIS operation staff and/or QSECOFR profiles with advance levels of authority, such as \*ALLOBJ, \*IOSYSCFG, \*JOBCTL, \*SAVSYS, \*SECADM, and \*SERVICE, will need to authenticate on sign-in using Multi-Factor Authentication (MFA).
  - Advanced user access should use multi-factor authentication (MFA) to the IBM-I. At a minimum these users should be multi-authenticated when accessing the County's network. If/when and MFA solution comes available it will be implemented on the IBM-I and managed by MCIS.
  - If MCIS purchases a common security solution for hosted LPARs, then MCIS will implement, monitor, and manage the solutions). Examples would be MFA, Exit Point Management, Audit, and Encryption software.
  - Above is available to remote support entities upon request.
- Manage IBM-i servers, and peripheral equipment:
  - MCIS controls the QSECOFR, DST, MCISADMIN, and access to MCISXXX profiles.



- Advanced access for MCISXXX profiles still has restricted access unless appropriate approval received by MCIS personnel to provide advanced access.
- County can designate individuals, from their IT department, who can request access to profiles such as QSECOFR. But they will place a helpdesk ticket to request access from MCIS and approval will be assessed to enable.

**Security Considerations/Handling – Remote Support**

- Managed IBM-i servers, and peripheral equipment:
  - MCIS controls the QSECOFR, DST, MCISADMIN, and access to MCISXXX profiles.
  - Advanced access for MCISXXX profiles still has restricted access unless appropriate approval received by MCIS personnel to provide advanced access.
  - County designate individual(s), that will need access to profiles such as QSECOFR, and will keep MCIS informed of how it is being used.



### **Level 3 – Advanced Support and Support of Non-MCIS Software:**

Tasks performed for hosted / on-site support but relate to managing more advanced operations tasks on IBM-i server(s) and monitoring/administering non-MCIS Software.

#### **Handle operational duties for non-MCIS Software.**

- County will provide training/documentation for:
  - Process for setup and changing of users with product owner on applications.
  - List of product owners (County user) and vendor contact information for support.
  - How vendors will request access to the application to support, such as access managed by county or MCIS coordinated.
  - Instructions on daily, weekly, monthly, yearly responsibilities County IT currently performs such as but not limited to running specific options within application, setting up users' access, clean-up steps, release/patch application, data clean-up/archiving tasks, and so forth.
- MCIS will perform patch/release of non-MCIS software, but need the following:
  - County will work with vendors to get access to their support portal, if applicable.
  - If vendor has capabilities, MCIS will set up alerts when new releases/patches come available.
  - Upon notification, MCIS will coordinate with the product owner(s) on how to proceed.
  - If an alert is not available, MCIS expects product owner to notify by placing a help desk ticket to when patches/releases are needed and where to obtain software release.

#### **Handling 3<sup>rd</sup> party providers (Vendor)**

- County ensures that vendor access is to the specific application only, and if vendor is granted higher level access that they are aware of County's security policies.
- Vendors will sign-in with their designated user profile and password, and change passwords based on county policy.
- Vendor's IBM-i profile will be disabled by default.
  - Product owner(s) will approve enabling IBM-i user profile by placing a help desk ticket to MCIS.
  - Product owner(s) can override this by placing a help desk ticket to notify MCIS what vendor profiles should remain enabled.
- MCIS can provide access one of three ways:
  - County provides vendors with VPN access to their connection point, and routes them to County's IBM-i partition. But, if a County has vendor's IBM-i profile always enabled, then MCIS has no way to monitor access and it becomes the full responsibility of County.
  - County users can provide access to their desktop device through virtual meeting capabilities.
  - MCIS staff will coordinate, as needed, vendor access through an MCIS supplied device:
    - County user must place a help desk ticket outlining purpose of request, date/time needed, Individual from vendor needing access contact information.
    - MCIS supplies a device for vendors to access County's partition.
    - MCIS is not responsible for actions taken by vendors regarding activities performed on the non-MCIS software.
    - If using an MCIS provided device, MCIS staff will monitor activity of vendor while accessing application through MCIS supplied device.
- Assist vendor in building a connection to the County's IBM-i partition from non-IBM-i servers (5250, ODBC), and setup of security on IBM-i to restrict access to vendor's specific data/objects associated with their application. MCIS is not responsible for providing data extraction/query assistance.
- Setup of nightly scheduled jobs needed based on instructions from product owner and/or vendor.
- Handle removal of software when no longer needed or used on IBM-i



### **Handling of Performance / Communication Issues**

- Upon identification or notification of an issue, the County users and/or County IT will report and log issues that are occurring with performance and details as requested by MCIS.
- MCIS will use this information to review the IBM-i performance tools to research the issue and provide directions to correct or where to go for additional assistance especially if it is related to non MCIS software performance.
- To resolve the issue MCIS may have to contract with an appropriate consultant (iTech, IBM, for investigation and will seek prior approval from County to move forward. This may be an additional charge to the county.
- If the issue is directly related to MCIS developed application performance, IBM-i hardware and/or Operating System, MCIS will coordinate the resolution. Otherwise, if related to third party(s) application(s), which are considered non-MCIS software and/or non-MCIS developed applications interfacing with MCIS developed databases and/or applications, then responsibility lies with the third party for coordination and resolution.

### **Security**

- MCIS will review security audit reports monthly. MCIS staff will recap issues for the IT Director, if any, and request action as needed.



#### **Level 4 – Remote Support and/or County Specific requests**

This section is not applicable to On-site Hosted counties.

#### **Level 2, 3 and 4 support disclaimers**

##### **MCIS does not provide the following for non-MCIS Software**

- “How to” or “Researching issues” with applications options, features, processes, procedures, or functions of that system. County users are required to work directly with the vendor.
- Securing private confidential/private data within non-MCIS software. Member can request MCIS to assist but requires county user(s) and/or vendor to identify what and how to secure.
- MCIS will perform a security assessment of IBM-i object settings as requested by county and determine recommendations.
- Creating and/or maintaining County developed applications/queries that use MCIS Software and/or non-MCIS Software tables.
- Creating/maintaining data imports/exports from/to non-MCIS applications and/or environments outside the IBM-i.
- Audit requests from County’s internal/external auditors that are beyond standard audit reports.
- Performing functions, a county user should be able to perform on applications.
- MCIS is not responsible for maintaining the code for special applications/process created on the IBM-i by Hosted Entity, unless specified in level 4 services, and/or non-MCIS software personnel such as but not limited to: user constructed queries; SQL calls from external source; Vendor/County constructed tables and/or tables views.

##### **Handling Vendor and/or County constructed views over MCIS Software tables.**

- MCIS assumes no responsibility for maintaining/managing custom views/tables when applying releases.
- After the MCIS software release is applied, the Vendor and/or County will review and recreate views as necessary.
- Vendor and/or County can have MCIS run a process to recreate views against MCIS table as an additional service but requires:
  - Application/script to be run directly on IBM-I.
  - Scripts to run provided and detailed instructions.
  - Contact information of the individual to pass on problems/issues that could occur in running of script (i.e name, phone number(s), email address).

##### **Handling of notifications to table changes and/or program/features changes to MCIS Software**

- Notification of database table changes, deletions, additions
  - Tables data elements changes/deletions/additions will be done at least 90 days in advance of project release date. Changes consist of length, data type, and/or edits built into the table definition for data elements (fields).
  - Existing tables view/index changes/deletions will be assessed individually to determine what advanced notice is required and approximate timeframe update will occur..
  - Existing table view/index additions will be part of the release notes with no advance notice.
- If changes to tables are mandated by Minnesota and/or Federal Legislative actions that require MCIS software to be changed in short cycle, the 90-day notification is waived.
- Upon notification, the County assumes responsibly to review/change their custom setups such as table views, custom code, queries, custom integration points and so forth, and/or coordinate information with 3<sup>rd</sup> party vendors.





**Service Level Agreements**

**Standard Service Coverage**

Monday through Friday, except holidays, 8:00 AM to 4:30 PM.

**Call Management Process**

- County users may continue to use their Help Desk to make a service request to MCIS or input a ticket directly to MCIS. The County will input a ticket into the MCIS Help Desk ticketing system to the functional area of "Host" with an appropriate amount of detail inputted into the description of the issue.
- Priority Codes outline severity of the problem and what the user should expect for response as follows:

Severity Level	Description	Response Time to Customer	Time to Resolve	Escalation Threshold
Critical	<b>Business Halted</b> –Critical component down or service are unavailable (all or a majority of users are unable to function, and no work around exists.	Within 1 hour	ASAP – Best Effort	2 hours
High	<b>Business Impacted</b> - Critical component (s) degraded. Large number of users or business critical functions affected, business processes can continue	Within 4 hours	ASAP- Best Effort	8 hours
Low	Limited to no degradation of service (non-critical problem or requirement, limited number of users or functions affected, business process can continue) without issue.).	48 hours	ASAP – Best Effort	96 hours

**After Hours Support - Standard**

MCIS does not have an after-hour alert system for emergency/critical issues, nor is it required. Performing patches/upgrades to OS or application software on Hosted Entities IBM-i server/partition, MCIS will coordinate installation to occur after normal business hours of County and MCIS. There are instances where the patch/fix is required by the County during the business day and MCIS will coordinate accordingly.

**After Hours Support for Special / Emergency Situations**

The County may request services after hours but will operate under these conditions:

- Non-emergency request for after-hours support will be scheduled in advance, and MCIS will determine availability and assess if billable.
- Emergency support
  - During Normal business hours contact MCIS Offices (218.326.0381)
  - For afterhours a county can request a calling tree provided under the assumptions
    - MCIS does not guarantee individuals are accessible immediately and message may have to be left on multiple phones.
    - If unable to reach anyone, staff will pick up message as soon as possible.
    - The MCIS individual reached will take it upon themselves to assemble appropriate resources and get back to County as soon as possible.
    - MCIS maintains the right to determine if the situation is billable.



## **EXHIBIT 2 – DEFINING MCIS SECURITY LEVEL 30/40**

Your security level is set as system value (QSECURITY). But just setting this value does not ensure that you meet the standard as defined in the current IBM Power I OS Version Security Guide. What is discussed below are excerpts from the security guide to help define the expectations for a minimum-security level being established for the hosted environment. Before changing a production system, read appropriate material in the IBM Power I security guide for migrating from one level to another, and the MCIS Security Guide.

### **Security level**

MCIS requires that hosted partitions have a security level of 30 or above on your system. The following requirements would meet security level 30 or 40:

- Both the user ID and password are required to sign on.
- Only someone with \*SECADM special authority can create user profiles.
- The limit capabilities value specified in the user profile is enforced.
- Users must be given specific authority to use resources on the system, which implies the users must be given specific authority to resources instead of users having all authority.
- Only user profiles created with the \*SECOFR user class are given \*ALLOBJ special authority automatically (see below "setting of default Special Authority")
- Use group profiles, and these groups are given \*USE authority to specific resources. Specific users are attached to these group profiles.
- Users are provided no special authority as defined below.
- No default sign-on - The IBM-i stops any attempt to sign on without a user ID and password that can be done on lower security levels.

MCIS will coordinate hosted entities implementation to comply, but require the following:

- County MIS will assign a staff member to assist MCIS in coordinating with users to understand access and assist with non-MCIS software.
- Commitment to complete the task within a 60-day period, unless mutually agreed upon to extend timeframes.

### **Default special authorities associated with security level 30 or 40.**

The system security level determines what the default special authorities are for each user class. When you create a user profile, you can select special authorities based on the user class. Special authorities are also added and removed from user profiles when you change security levels.

These special authorities can be specified for a user through proper authorization controls implemented by the county:

\*ALLOBJ - All-object special authority gives a user authority to perform all operations on objects.

\*AUDIT - Audit special authority allows a user to define the auditing characteristics of the system, objects, and system users.

\*IOSYSCFG - System configuration special authority allows a user to configure input and output devices on the system.

\*JOBCTL - Job control authority allows a user to control any jobs in subsystems and printing on the system.

\*SAVSYS - Save system authority allows a user to save and restore objects.

\*SECADM - Security administrator authority allows a user to work with user profiles on the system.



## Minnesota Counties Information Systems

413 SE 7th Avenue, Grand Rapids, MN 55744  
Phone 218-326-0381

\*SERVICE - Service authority allows a user to perform software service functions on the system.

\*SPLCTL - Spool control authority allows unrestricted control of output queues on the system.

You can also restrict users with \*SECADM and \*ALLOBJ authorities from changing this security related system value with the CHGSYSVAL command. You can specify this restriction in the System Service Tools (SST) with the "Work with system security" option.

Table 2 shows a preferred approach to granting special authorities by each user class. The entries indicate that the authority is given at all security levels, limited/controlled to a few, or not at all.

Special authority	Recommended Granting Special Authority based on Types of Work				
	*SECOFR	*SECADM	*PGMR	*SYSOPR	*USER
*ALLOBJ	All				
*SECADM	All	All			
*JOBCTL	All			All	
*SPLCTL	All				
*SAVSYS	All			All	
*SERVICE	All				
*AUDIT	All				
*IOSYSCFG	All				

Hosted counties that have third parties, such as non-employees, vendors, consultants, and so forth, accessing their partition need to establish procedures following these points:

- Assign unique user profile on IBM-i for 3<sup>rd</sup> parties for auditing/tracking purposes.
- Require 3<sup>rd</sup> party to connect into the County's network through a secure connection. Then routed to the IBM-i where access is limited to the software functions the County has approved them access for.
- Profile with special authorities, such as \*ALLOBJ, \*IOSYSCFG, \*SECADM, and/or \*SERVICE, then independent access should not be allowed. Instead, set up a virtual meeting where County users, County MIS or MCIS can monitor what is occurring. If MCIS is monitoring, a help desk ticket with county authorization is required.
- If a user profile access is infrequent (as defined by county), then disable that user profile by default and enable when requested.

Instances where applications need to interface via an internet connection directly to hosting entities LPAR, and/or from the LPAR via internet connection to another web services/server (i.e. PRISM, E-Crv, printing tax statements from a web site, payroll self-service, and so forth):

- Utilize a secure connection (TLS/SSL) between entity and hosting center, especially when transmitting confidential/private data.
- Limit authorities of user profiles coming into the LPAR, and access to objects.
- For accessing into Hosted Entity's LPAR
  - The hosting center network team will assign a public IP address for the LPAR.
  - Where possible restrict access to incoming IP address, URL, domain name, and/or route to a specific application and only allows that application to run.
  - Use the IBM-i profile assigned to the application, and that profile should not be allowed to sign in interactively.



## **Exhibit 3 - MCIS Security Committee Charter**

### **Purpose**

The MCIS Security Committee's (the "Committee") primary purpose shall be to act on behalf of the MCIS Board in fulfilling the Board's oversight responsibility with respect to the Company's information technology use and protection. This document describes the compositions, functions, and authorities granted to the committee.

### **Committee Composition**

- MCIS Executive Director – serving as chair of committee.
- MCIS Software Development Manager(s)
- IBM-i Network Administrator(s)
- As Needed
  - Contracted desktop, server, networking services provider, currently VC3
  - MCIS Executive Committee and/or MCIS Board designees
- When hosted environment is impacted.
  - Facility provider (Itasca County)
  - Member County IT Staff as defined by member's IT Director
  - Member County's Primary Board designee

### **Committee Functions**

- Data Governance – To provide oversight of policies, procedures, plans, and execution intended to provide security, confidentiality, availability, and integrity of the information.
- Information Technology Systems – To oversee the quality and effectiveness of the company's policies and procedures with respect to its information technology development and support activities as it relates to the MCIS developed applications, accessing MCIS members' environment, including privacy, network security and data security.
- Incident Response – To review and provide oversight on the policies and procedures of the Company in preparation for responding to any material incidents.
- Disaster Recovery – To review periodically the organization's disaster recovery capabilities.
- Compliance Risks and Internal Audits – To oversee the management of risks related to the organization's information technology systems and processes, including privacy, network and data security, and any internal audits of such systems and processes.
- Advisory Role – To review the organization's information technology strategy or programs relating to new technologies, applications, and systems.
- General Authority – To perform such other functions and to have such powers as may be necessary or appropriate in the efficient and lawful discharge of the foregoing.

### **Committee's Authority**

- The Committee shall have full access to all books, records, facilities, and personnel as deemed necessary and/or appropriate by any member of the Committee to discharge responsibilities hereunder.
- To expediate initial investigation the MCIS Executive Committee is pre-approved by the MCIS Board to authorize up to \$25,000 of reserve funds to engage special legal, financial, cybersecurity, publicity consultants, or other advisors or consultants as it deems necessary or appropriate in the performance its duties.



**Minnesota Counties Information Systems**

413 SE 7th Avenue, Grand Rapids, MN 55744

Phone 218-326-0381

- For unbudgeted expenses beyond \$25,000
  - The Security Committee will prepare a proposal of need.
  - MCIS Executive Committee will make a recommendation to allocate additional funds, and/or how to expense may be allocated to individual joint power's members.
  - MCIS Board meeting will be assembled expeditiously by MCIS Executive Committee for approval to proceed.

The Security Committee shall have authority to require that any of the personnel, counsel, accountants (including independent outside auditors), or any other consultant or advisor, attend any meeting of the Committee or meet with any member of the Committee or any of its special, outside legal, accounting, or other, advisors or consultants.

The approval of this charter by the Board shall be construed as a delegation of authority to the Committee with respect to the responsibilities set forth herein.

On July 27, 2023 the MCIS approved the MCIS Security Committee Charter

Signed: Amber Peratalo  
Amber Peratalo, Chairperson

Attest: Nancy Nilsen  
Nancy Nilsen, Secretary

08/10/2023

# Signature Certificate



Envelope Ref:406403a5c89461370e16e25264255d258bf97eb1

Author: Lyle Eidelbes

Creation Date: 10 Aug 2023, 16:04:26, CDT

Completion Date: 11 Aug 2023, 10:24:48, CDT

## Document Details:



Name: Exhibit 3 - MCIS Security Committee Charter-R20230810

Type:

Document Ref: 91edb0f1aa7a0f00d451ef8df3d447b2f3f74eab82eeb93a1fa22e5d00258654

Document Total Pages: 2

## Document Signed By:

Name: Nancy Nilsen  
Email: nilsenn@stlouiscountymn.gov  
IP: 71.13.38.43  
Location: DULUTH, MN (US)  
Date: 10 Aug 2023, 17:01:42, CDT  
Consent: eSignature Consent Accepted  
Security Level: Email

*Nancy Nilsen*

Signer ID :TNTFZXFM37...

Name: Amber Peratalo  
Email: amber.peratalo@co.itasca.mn.us  
IP: 207.171.101.27  
Location: GRAND RAPIDS, MN (US)  
Date: 11 Aug 2023, 10:24:48, CDT  
Consent: eSignature Consent Accepted  
Security Level: Email

*Amber Peratalo*

Signer ID :GF2PTABBIU...



**Document History:**

Envelope Created	Lyle Eidelbes created this envelope on 10 Aug 2023, 16:04:26, CDT
Invitation Sent	Invitation sent to Amber Peratalo on 10 Aug 2023, 16:11:07, CDT
Invitation Sent	Invitation sent to Nancy Nilsen on 10 Aug 2023, 16:11:07, CDT
Invitation Accepted	Invitation accepted by Nancy Nilsen on 10 Aug 2023, 16:59:38, CDT
Signed by Nancy Nilsen	Nancy Nilsen signed this Envelope on 10 Aug 2023, 17:01:42, CDT
Invitation Accepted	Invitation accepted by Amber Peratalo on 11 Aug 2023, 10:24:30, CDT
Signed by Amber Peratalo	Amber Peratalo signed this Envelope on 11 Aug 2023, 10:24:48, CDT
Executed	Document(s) successfully executed on 11 Aug 2023, 10:24:48, CDT
Signed Document(s)	Link emailed to <a href="mailto:amber.peratalo@co.itasca.mn.us">amber.peratalo@co.itasca.mn.us</a>
Signed Document(s)	Link emailed to <a href="mailto:nilsenn@stlouiscountymn.gov">nilsenn@stlouiscountymn.gov</a>
Signed Document(s)	Link emailed to <a href="mailto:lyle.eidelbes@mcis.cog.mn.us">lyle.eidelbes@mcis.cog.mn.us</a>



## **Minnesota Counties Information Systems**

413 SE 7th Avenue, Grand Rapids, MN 55744  
Phone 218-326-0381

---

### **EXHIBIT 4 – NIST Special Publication 800-88 Revision 1**

These specifications are maintained by the National Institute of Standards and Technology. The document is currently 64 pages and provides all the information on guidelines for data sanitization. To obtain the current version it is suggested you cut and paste this URL below into your browser window. Otherwise, contact MCIS to obtain a copy and email to you.

URL <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>