Goodhue County
Minnesota

TECHNOLOGY COMMITTEE MEETING

ADMINISTRATION CONFERENCE ROOM
GOVERNMENT CENTER, RED WING

OCTOBER 26, 2023
8:30 A.M.

1. **Broadband Update**
2. **IT Department Staffing Update**
3. **County IT and AMC - MNCITLA**

   Documents:

   MNCITLA LEGISLATIVE PLATFORM 2024.PDF
   AMC COUNTY CYBERSECURITY 101_20230925.PDF

4. **2023 IT Projects Update**

   Documents:

   10.26.2023.TECHNOLOGY_PROJECTS_2023.PDF

5. **Q & A**
6. **Next Meeting Date & Time**

Minnesota County Information Technology Leadership Association

MNCITLA 2024 Legislative Platform

The Minnesota County Information Technology Leadership Association (MNCITLA) is a voluntary membership association consisting of over 60 counties from around the state.

MNCITLA's purpose is to support Minnesota county information technology leaders through collaborative communication between counties, state agencies, the Legislature, and public sector organizations.

MNCITLA prides itself on successfully integrating counties of all sizes into an active organization. Our goals include providing education and advocacy that reinforce how foundational information technology is to every county function. We believe that IT must be valued as an integral part of public service and governance, as opposed to merely technical support.

In 2019, MNCITLA formally affiliated with the Association of Minnesota Counties (AMC) to establish an advocacy presence at the State Capitol and to collaborate more effectively across county professional associations.

Cybersecurity

Minnesota's citizens rely on their counties to provide election services, vital records management, public health and humans services, public safety, road and bridge maintenance, property records, environmental resources, waste disposal, and other essential services. County governments rely completely on secure, interoperable technology systems to deliver these services. These systems link federal, tribal, state, county, and other local governments together, presenting challenges and opportunities. The need for interconnected technology systems between units of government means that a security risk at one city, county, state agency, or contracted vendor becomes a threat vector for all.

- MNCITLA supports the Legislature working with agencies, local governments, and other stakeholders to develop an ongoing, state-funded cybersecurity grant program. This program would build on the work of the State and Local Cybersecurity Grant Program and other federal programs.
- MNCITLA supports and prioritizes greater collaboration between counties and state agencies on cybersecurity efforts including security event monitoring, shared trainings, outreach programs, vulnerability assessments, and incident response.

Artificial Intelligence

Artificial Intelligence (AI) and Machine Learning has evolved to allow state and county government to adopt this tool into their day-to-day operations. MNCITLA view County Governments ability to use generative AI as an opportunistic tool that may be adopted by an entity to fill the gap of meeting citizen expectations and to fill gaps as the workforce resources decline. MNCITLA supports the use of AI in government but believes strong guardrails are necessary to protect sensitive data and mitigate inaccuracies from the outputs of generative AI tools.

- MNCITLA supports creating a state-driven AI data warehouse for data sharing to local governments as well as analytics to help with forecasting.
- MNCITLA supports policies preventing county data being collected into AI tools.
- MNCITLA supports convening a state and local government working group with the intention of creating comprehensive AI data use policies.

Next Generation 9-1-1

Next Generation 9-1-1 (NG911) technology is necessary for the safety of our communities so that individuals can be located with a high degree of accuracy when calling from a mobile device, or texting 911. This technology will be implemented by the Minnesota Department of Public Safety in response to the NG911 Advancement Act of 2012. MNCITLA recognizes the enhanced partnership between County Geographic Information Systems (GIS) mapping and 911 services, due to counties being tasked with building the emergency management maps that are foundational to NG911 technology. Long-term maintenance and protection of NG911 infrastructure will also be the responsibility of county governments.

- MNCITLA supports dedicated funding for current County Geographic Information System mapping efforts related to NG911 rollout.
- MNCITLA also supports ongoing, dedicated funding to meet future cybersecurity and infrastructure needs of NG911.

IT Workforce and Training

Minnesota will need to fill 45,000 tech jobs and 6,500 IT jobs by 2032, according to a recent study by the Minnesota Technology Association. The same study estimates Minnesota will only produce 6,600 new tech workers by 2032. Competition between private entities and Counties for IT workers is already fierce. Educating and training thousands more technology and IT workers ensures fewer vacancies on County IT staffs.

- MNCITLA supports efforts to increase the availability of computer science courses at secondary and post-secondary institutions.
- MNCITLA supports efforts to develop training or apprenticeship programs that upskill non-IT workers pursuing careers in IT.

Broadband

Broadband is an integral part of everyday life, yet nearly 10% of all Minnesotans—and a 25% of rural Minnesotans—don't have access to quality high-speed broadband service. Every aspect of today's world—workforce, telehealth, education, business, and agriculture—depends on a reliable broadband connection. Expanding broadband accessibility and affordability will allow local governments to provide more effective and efficient services to our communities in the future.

- MNCITLA supports equity and access to affordable broadband service and infrastructure in Minnesota.
- MNCITLA supports legislation that would provide adequate and continuous funding for the Border-to-Border Broadband Development Grant Program.
- MNCITLA supports the goal of statewide deployment of modern, scalable broadband networks that meet or exceed state statutory speed goals.

Data Management

Counties create and are entrusted with a significant amount of sensitive data. As the data generated, collected, and maintained by counties grows, so does the challenge of securing, storing, and sharing data.

- MNCITLA supports clarification and simplification of existing data practices statutes.
- MNCITLA supports funding allocations for county governments to offset the growing costs associated with securing, storing, and sharing government data.

County-State IT Collaboration

County IT departments face challenges when administering state and federal services to Minnesota's residents. County IT departments and their leaders must have public sector-specific knowledge to navigate the challenges of technical implementation these services require, which can present a barrier in understanding for those outside of public-sector IT. Greater collaboration, visibility, and understanding between counties and state officials is necessary for efficient operation of county-managed systems.

- MNCITLA's goal is to provide information to elected officials and state agencies in an approachable and understandable way.
- MNCITLA supports reducing overall costs through greater collaboration between government entities including agency-sponsored, county-managed systems.

Technology Procurement Process

The procurement process in Minnesota provides competition and essential transparency when using taxpayer dollars. As county governments utilize more complex technology, the limitations of Minnesota's procurement process in technology acquisition have become evident, particularly when county business needs change.

- MNCITLA supports modifications to the procurement process that allow for more innovation, collaboration, and adaptability in technology acquisition.

Resources for Digital Accessibility

Digital resources have become integral in how citizens understand and interface with their county governments. As these technologies continue to expand, MNCITLA understands this increase in interaction and transparency requires a simultaneous focus on digital accessibility and inclusion. The Rule to Improve Online Accessibility announced by the Department of Justice further underscores that Counties will need to implement specific technical standards to remain in compliance with Title II of the Americans with Disabilities Act.

- MNCITLA supports funding for implementing digital accessibility standards.

For additional information, please contact MNCITLA Executive Director, Nathan Zacharias at nzacharias@mncounties.org or 715-222-2824.

Association *of* Minnesota Counties

COUNTY CYBERSECURITY 101

Fall 2023

TABLE OF CONTENTS

Disclaimers

Resources compiled by and narrative written by the Association of Minnesota Counties' Cybersecurity Task Force. References and hyperlinks to resources developed by MCIT, CISA, NACo, NYSAC, and many more included herein. This document does not delineate all cybersecurity requirements as specifically required of counties by state and federal agencies, such as the Minnesota Bureau Criminal Apprehension's (BCA) Criminal Justice Data Communications Network requirements or the FBI's CJIS Security Policy. Please consult your county officers, staff, legal counsel, and agency partners when assessing requirements. This document is meant for informational and educational purposes.

EXECUTIVE SUMMARY

This document is meant to serve as a call to action, encouraging county policymakers, administrators, and IT leadership to engage with each other on the development of county-wide cybersecurity policies, procedures, and infrastructure, to meet the rising threat of cyberattack.

A county's information technology (IT) infrastructure is essential for providing core county services that function across all service areas. The digital safety, integrity, and availability of the infrastructure is a top priority to ensure the core services are provided to our community. Underprioritizing cybersecurity can lead directly to operational failure, extreme and sudden financial burden, and erosion of the public trust at the hands of a cyberattack operating from anywhere in the world. Due to the interconnected nature of the current day, a cybersecurity breach in one organization can sometimes expose many others – from school systems to counties to state agencies and beyond – so every organization has a responsibility to the larger community to readily address the modern threat of cyberattack. Moreover, ignorance of cybersecurity risk is not legally defensible in the event of a lawsuit.

In September of 2022, the Association of Minnesota Counties (AMC) assembled a Cybersecurity Task Force (AMC CTF; "Task Force") to assess the statewide county cybersecurity posture at a high level. The Task Force acknowledges the need and opportunity for pursuing state-level policy and programs to help address this statewide issue. The Task Force appreciates that no matter how much action the state takes, county-level action is necessary for a cyber-secure Minnesota. To this end, the Task Force developed this document to help bolster Minnesota counties' "cyber readiness" and elevate the digital safety of the public and the dependability of county services in the face of cyberattacks.

In this document, you will find an explanation of the cyber threats that counties face, an evergreen approach to managing the risks of exposure to ever evolving cyberattacks, and some next steps to take today to better protect your county.

The bottom line: Cybersecurity is a shared duty across leadership and staff within each county. Your county's board, administration, and IT leadership must work together in earnest to design cybersecurity policies, procedures, and infrastructure for implementation across all county departments. The threat of cyberattack is real and present, and every county must take part to create a stronger cybersecurity posture for Minnesota as a whole.

Cyberattacks on Counties

In recent years, Minnesota counties have faced an increasing number of cyberattacks. These attacks have disrupted county business, halted service to the public, burdened county governments with hefty ransoms and cyber-attack postmortem costs, and – in some cases – damaged the reputation of counties and county officials.

Cyberattacks are malicious attempts by cybercriminals to access the infrastructure using a personal computer, a connected device, an account, or other networked gear for the purposes of causing a disruption, traversing to a larger target, misdirect funds, collecting intelligence for further actions, stealing, spying on, or exposing private data, holding data for ransom, rendering the computer/device/network unavailable, fraudulently redirecting funds, or hijacking the computer/device/network for use in further attacks, among other nefarious motivations.

Cyberattacks can require expensive and time-consuming response efforts. This leads to cause serious damage to the public trust. Some examples of the types of cyberattacks and the risks they pose are described below.

Sabotage & Hijacking

- Attackers take important county functionalities offline or hijack county website(s).
  - Impact to 911 / emergency services.
  - Impact county communications, for example office phones, email systems, and websites may go down and be inaccessible to employees and the public.
  - Inability to receive/send payments, taxes, etc.

Fraud & Impersonation

- Attackers use data from hidden spyware on county systems to target payment patterns and fraudulently insert familiar-looking payment requests into billing cycle.
  - Payments can be diverted with no ability to retrieve funds.
    - Substantial levy impacts – in some cases, significant proportions of annual property tax levy for large payments toward capital projects.
- Attackers can impersonate a third party, a county partner, or a county employee to social engineer information, mis-direct payments, or cause havoc to systems and services.

Data Breach

- **Attackers access sensitive data:** Social security numbers, birth dates, banking information, program enrollment of vulnerable persons, etc.
  - **Private data accessed:** County must send notification to affected persons and voters, typically via letters signed by administrator and/or officials.
    - Depending on the data and size of the breach, credit monitoring subscriptions will also be made to the breached persons at the county expense.

    - **Ransomware attack:** Attacks can remove, alter, or lock data from county systems. It will deny county access to own systems and demand payment for restoration of access and/or return of removed data.
        - Ransom attack presents a lose-lose conundrum: Paying a ransom does not guarantee you will get your data back as it was.
        - The integrity of data is lost.
        - The integrity and reputation of the county will be evaluated by the public and trust can be lost based on the county response to this type of an attack.
        - Whether or not ransom paid, attack postmortem expenses and/or data restoration takes a significant amount of time and money.
        - **Some data lost permanently:** Impacts service delivery, license status, property tax collection, etc.
- Your county's information security is heavily interrelated with your county's cybersecurity. The clearest example is how too long of a data retention schedule – say, several years' retention of most or all data – can balloon your county's risk by growing the body of data that must be classified, archived, and ultimately protected against attack.

Liability & Insurance Coverage

- Cybersecurity insurance premiums are rising, and attacks continue to mature and grow.
- A low "cyber readiness" may impact a county's ability to secure insurance coverage or may narrow terms of coverage offered.
- Insurance is a response effort and prioritizing the counties cyber posture will reduce the likelihood of requiring a large insurance policy.

Cyberattacks: The Aftermath

Whichever kind of attack befalls a county, the more severe attacks, especially on an unprepared county, can prompt substantial public response. County personnel and officials may find themselves inundated with complaints via phone, voicemail, email, the public comments portion of county board meetings, and more. This sort of response can represent a breach of the public trust, which can take a long time – often more than an election cycle – to repair.

Preparedness for Attacks and Improving Response

Counties must review and update the way they approach digital safety and cybersecurity practices. Cybersecurity is not a specialized program that falls as one of many responsibilities of an IT department. Rather, a county's "cyber readiness" must be approached strategically, holistically, and systematically with respect that this is a central, core function to deliver services across the county. The ongoing efforts to track, monitor, and achieve the county's readiness plan is a way to be ready to respond to a cyberattack. While it is typical that an I.T. department may track, lead, and maintain the program for the county, all county departments and employees play a part of ensuring the governance is followed, communication is sent and received to all appropriate parties, and that testing of the response plan is executed.

Risk Management Approach to Cybersecurity

County boards and administrators are already familiar with applying risk management to other aspects of county business. Approaching county cybersecurity from the same perspective would identify and address key areas of risk and the liability posed by the threat of cyberattacks.

A risk-based approach to cybersecurity follows the steps described below:

1. **IDENTIFY RISKS – Audit your county's cybersecurity posture.**
    a. Determine your assets and identify the risks associated with each.
        i. Assets include physical property/hardware (computers, phones, switches, routers, etc.), software/services (cloud hosted and county hosted), employees, and vendors/contractors.
    b. What county services could be interrupted by a cyberattack? Said differently, what county services would halt if the county became unable to accept or receive payments? Phone calls? Emails?
    c. What kind of attack could disable emergency communications / dispatch?
    d. What private data does the county store that could be subject to a cyberattack?

2. PRIORITIZE & CATEGORIZE RISKS

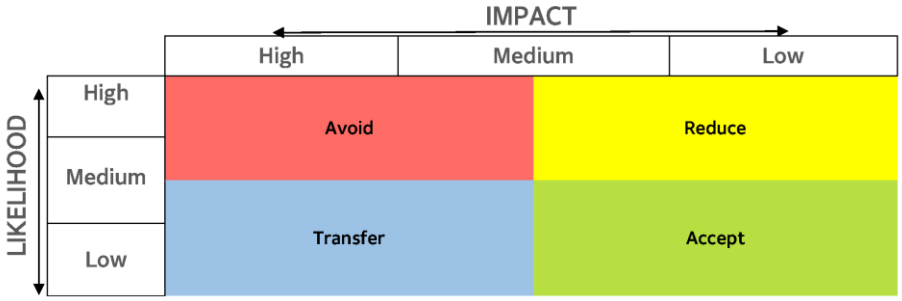
a. Prioritize your risks listed in Step 1 as critical or non-critical. You may also include the Service type, business need, and data type (type of data transmitted, stored, accessible, etc.)
b. Apply a standard mapping tool to each risk to determine the likelihood vs Impact of the risks. See sample.
c. Provide acceptable timeframes as to how long a service can be down and the cost of the service being out.
d. What services are essential to basic county function?
e. If taken offline by a cyberattack, lack of which services could pose harm to county residents and visitors? To county partner organizations?
f. What data poses the greatest liability (financial and reputational) if stolen or accessed in a cyberattack?
g. What areas are most susceptible to human error / deception of county personnel by fraudulent / phishing cyberattack?

LIKELIHOOD	IMPACT: Minor	IMPACT: Moderate	IMPACT: Significant
Likely	Medium	Medium High	High
Possible	Low Medium	Medium	Medium High
Unlikely	Low	Low Medium	Medium

3. PLAN RISK MITIGATION ACTIONS

a. For each risk:
   i. Do you accept the risk? If so, how will you reduce risk?
   ii. Do you mitigate the risk? How?
   iii. Do you transfer the risk? If so, who to and how? Vendor, insurance, etc.
   iv. Do you remove the asset to remove or reduce the risk?

b. What standards and procedures could be established to prevent service interruption or unauthorized access? Is there a corresponding need for new funding, equipment, training, staff capacity, or other support?
c. What procedures are in place to identify, contain, assess, and recover from cyberattacks? Which parties internally are responsible for each step? Who, externally, can responsible parties contact for assistance and reporting? Is there a corresponding need for new funding, equipment, training, staffing capacity, or other support?
d. What liabilities can be covered through purchasing cybersecurity insurance? Which liabilities are not covered or more costly to cover than to mitigate?
e. For any funding needed, is the need for funding ongoing? Cyclical? What funding sources are feasible and dependable?
    i. Consistent funding is essential and currently does not exist at the state level for county use. Counties need to plan for and fund cyber readiness as it does any other critical infrastructure, recognizing that state or federal support may be sporadic, but the threat of cyberattack is constant.



4. IMPLEMENT MITIGATION CONTROLS

a. Create or update training materials, procurement processes, inventory processes, employee preparedness tests, payment procedures, mark new devices/applications with sunsetting software support for upcoming year, etc.
b. Allocate and spend funds on identified investments and risk mitigation measures.
c. For controls identified and where appropriate, identify metrics by which to measure control success/adherence.

5. MONITOR ACTIVITY & ASSESS CONTROLS

a. Ongoing year-round: Conduct employee training, employee preparedness tests, sunset unsupported devices/applications on schedule, sunset unused/shared user/vendor accounts, track and measure user activity and access where possible, etc.
b. Update Security Information & Event Management (SIEM) software as necessary for any new metrics developed.
c. As metrics indicate, identify risk areas not being improved by implemented controls; elevate for out-of-cycle reconsideration or course-correction as appropriate.
d. Continue to identify risks, prioritize, and manage risk register (descriptive list of known risks).

Next Steps: Risk Mitigation Controls

Below are some high-value controls that a county might implement to mitigate risks in the event of an attack. These steps represent a baseline for the time of publication of this document; updates beyond those listed below may be necessary as may be identified by the cyclical risk assessment process identified above in future years.

- **ROLES & RESPONSIBILITIES**
  - Develop a policy to continuously manage and monitor risks and identify the best process for doing this.
  - Develop ongoing monitoring and maintenance duties; assign responsibilities and verify adherence to policies and procedures.
  - Develop emergency response / cyberattack procedures; assign responsibilities and test preparedness.
  - Develop and update cybersecurity policies addressing the topics below:
    - Acceptable use (of county network and/or devices)
    - Asset management
    - Change management
    - Access control
    - Incident management
    - Data classification management
    - Network management
    - Physical security
    - Security training and awareness
    - Vulnerability management
    - Remote work / work from home
    - Third party requirements
- **PERIMETER PROTECTIONS**
  - Firewall
  - Web filter
  - Intrusion detection system (IDS) / Intrusion prevention system (IPS)
- **COMMUNICATIONS CONTROLS**
  - Spam blockers
  - Filtering
  - Access
  - Domain-based message authentication, reporting, and conformance (DMARC)
- **EMPLOYEE PREPAREDNESS TRAINING & TESTING**
  - Annual (at least) phishing, fraud, internet use training, folded into “slips-trips-falls” programming.
  - Automated or vendor-driven intermittent phishing / fraud testing (more frequent than annual)

- Tabletop exercises
- In-depth annual training for positions with higher levels of responsibility for data management, cyberattack incident response, etc.

- **INTERNAL ACCESS CONTROLS & ACTIVITY MONITORING**
  - Data retention policy up-to-date and in-use
  - Integrated Resource Plan (IRP) up-to-date and in-use
  - Continuous & automatic data backup – offsite?
  - Multi-factor authentication
  - Endpoint (device) protection – updated antivirus software, automated remote patching, etc.
  - Standard configurations – devices must be patched, supported, and approved to access network.
  - User-level access controls & activity monitoring
  - Security Information & Event Management (SIEM) service
  - Controls and/or monitoring for third parties accessing network or devices.

Immediate Actions for Your County

If you have not already implemented the items below in your county, please engage your board, administration, and IT leadership together to do so now!

- Conduct regular security training and testing. User error is one of the greatest areas of cybersecurity risk, so training all county personnel to detect and avoid phishing scams, suspect links or files, and other common methods of attack is vital.
- Multi factor authentication. If you cannot arrange for all staff, prioritize privileged users to systems and infrastructure.
- Limit systems from communicating outside of the USA and Canada.
- Back up your systems offsite.
- Update network infrastructure, keep software patches updated.
- Manage remote access abilities.
- Encrypt your data.
- Develop an incident response plan and test.
- Require strong and unique (not shared) passwords for all county network users.
- Establish approval process for accounts with elevated access.
- Annually review accounts, elevated accounts, access permissions, etc.
- SAMPLE COUNTY CYBER SECURITY POLICY

SAMPLE CYBERSECURITY POLICY

1. Policy Statement

Sample County acknowledges its obligation to its residents, visitors, and persons interacting with county services to establish and uphold comprehensive cyber security systems and practices.

To protect the security of all data owned or kept by Sample County and to maintain the functional integrity of all Sample County information systems and networks, Sample County will ensure its cyber security posture matches its risk profile through county-wide standards, staff and personnel training program(s), and software and hardware update schedules.

This policy applies to all employees, elected and appointed officials, contractors, and vendors, and other third parties that access data held or managed by Sample County, or the software, hardware, and systems that store or access said data.

2. Definitions

"Software" means all scripts, applications, APIs, cloud-based services, software firewalls, and other digital products or systems used by Sample County or any third party operating on behalf of or in agreement with Sample County.

"Hardware" means all user devices – phones, tablets, laptops, desktops, etc. – as well as all network devices – servers, routers, modems, Wi-Fi boosters or access points, ethernet bridges, switches, gateways, hardware firewalls, etc. – used by Sample County or any third party operating on behalf of or in agreement with Sample County.

"System" or "Systems" – especially in the context of "software, hardware, and systems" – generally refers to information systems and/or communication systems used by Sample County or that interact with information systems and/or communications systems used by Sample County.

3. Cyber Security Requirements

Sample County must establish, maintain, and update county-wide standards, procedures, and programs listed and described below. These requirements apply to all employees, elected and appointed officials, contractors, and vendors, and other third parties that access or use Sample County data, electronic systems, and/or equipment.

3.1 Cyber Security Risk Assessment Standards

Sample County shall establish a bi-/annual cyber security risk assessment process. All software, hardware, systems, and third-party partnerships related to information systems are subject to

cyber security risk assessment before they can be approved by Sample County to store or access data held or managed by Sample County.

3.2 Cyberattack Response Standards

Sample County shall establish detailed procedures for use upon detection of cyberattack to log, define, scope, track, prioritize, and resolve all known types of cyberattack for which Sample County is at risk for. The procedures shall identify the responsible persons for each component of the procedures. The procedures shall determine what software, hardware, systems, and procedures must be re-assessed for potential changes to prevent similar future cyberattacks. The procedures shall determine the extent to which notification of state agencies and the public is required, and the extent to which notification of state agencies and the public is prudent.

3.3 Activity Monitoring Standards

All software, hardware, and systems that store or access data held or managed by Sample County must be monitored for threats and cyberattacks.

3.4 Software and Hardware Standards and Vulnerability Testing

All Sample County software, hardware, and systems that store or access data held or managed by Sample County must be tested and assessed for vulnerability to cyberattack. Identified vulnerabilities must be prioritized based on risk level and be addressed promptly. All software, hardware, and systems that store or access data held or managed by Sample County must be assessed for necessary updates, replacement, and usage restrictions on a routine and timely basis. Only software, hardware, and systems approved by Sample County may be used to access data held or managed by Sample County.

3.5 Minimum Data Standards

Data held or managed by Sample County shall be stored on actively managed centralized storage devices and systems. Sample County will establish standards for: data backup; data recovery; records retention & disposal; device decommissioning, reuse, recycling, or disposal; software decommissioning; and more.

3.6 Network Security, Information Technology (IT) Systems, and User Identification Standards

Physical and/or digital access to Sample County networks and all data held or managed by Sample County software, hardware, and systems shall be restricted. Exceptions will be made

strictly as necessary to perform essential duties and in such a manner as to not jeopardize Sample County cyber security standards. All connections granting physical and/or digital access as described above must identify the user. A given user must have one identity (matching ID value, linked ID values, or similar method) across Sample County software, hardware, and systems. In the event of a breach enabled by a given user/identity Sample County must be able to, in a uniform manner, remove or limit that user/identity's access to data held or managed by Sample County across Sample County software, hardware, and systems.

3.7 Cyber Security Training and Testing Standards

Sample County will implement, maintain, and administer training and simulated testing standards and programs for County employees, elected and appointed officials, contracted workers, and any other user accessing data held or managed by Sample County. Failure to meet these standards may result in personnel policy violation(s), termination of employment or contracted agreement, or other sanctions as appropriate.

4. Implementation Responsibility

Implementation of this policy shall be the responsibility of the County Administrator acting as the agent of the Sample County Board, in consultation with the Sample County Cyber Security Committee and the Sample County IT Director and/or Chief Information Security Officer.

ACRONYMS & DEFINITIONS

- BCA CJDN – Minnesota Bureau of Criminal Apprehension's Criminal Justice Data Communications Network
- CISA – Cybersecurity and Infrastructure Security Administration
- CJIS – United States Department of Justice / Federal Bureau of Investigation Criminal Justice Information Services
- DPS-ECN – Minnesota Department of Public Safety, Emergency Communications Networks Division
- EI-ISAC – Elections Infrastructure Information Sharing and Analysis Center
- IT – Information technology
- MCIT – Minnesota Counties Intergovernmental Trust
- MNCITLA – Minnesota County IT Leadership Association
- MS-ISAC – Multi-State Information Sharing and Analysis Center
- NACo – National Association of Counties
- NIST – National Institute of Standards and Technology
- NYSAC – New York State Association of Counties

RESOURCES

Guidance Documents

- Cybersecurity Self-Assessment (MCIT)
- Cyber Essentials Starter Kit (CISA)
- Cybersecurity Priorities Kit (NACo)
- Cybersecurity Primer for Local Governments (NYSAC)
- PSAP Cybersecurity Assessment Project Update (DPS-ECN)
- MN Judicial Branch Cybersecurity Policy 2018

Other Resources

- BCA CJDN Security Standards
- CJIS Security Policy
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC)
- Minnesota County IT Leadership Association (MNCITLA)
- National Institute of Standards and Technology (NIST)

ACKNOWLEDGEMENTS

Thanks to the AMC Cybersecurity Task Force members, advisors, and AMC staff for their thoughtful input and meaningful time set aside to diagnose and tackle this very important issue. Special thanks to the Subgroup members, marked with an asterisk below, who met further to aid the development of this document:

Eric Brown, Chief Information Security Officer, Ramsey County

Matthew Cook, Project Manager, AMC

Lyle Eidelbes, Executive Director, MCIS

Neal Gaalswyk, Commissioner, Cass County

Mike Gamache, Commissioner, Anoka County

Karri Harvey, IT Director, Blue Earth County; MNCITLA Treasurer

Kersten Kappmeyer, Administrator, Pope County

Bill Keller, Central Services Director, Anoka County

Mike Koehler, CPT

Larry Lindor, Commissioner, Pope County

David McKnight, Director of Enterprise Finance and Information Services Division, Dakota County

Lisa Meredith, Executive Director, MnCCC

Gene Metz, Commissioner, Nobles County

Amy Middendorf, IT Director, Morrison County; MNCITLA Vice Chair

David Minke, County Administrator, Pine County

Eric Nerness, Director of Claims, MCIT

Chris Pelzer, County Coordinator, Todd County

Julie Ring, Executive Director, AMC

Chris Stauffer, IT Director, Roseau County

Jack Swanson, Commissioner, Roseau County

Nathan Zacharias, Technology Policy Analyst, AMC; MNCITLA Executive Director

Special thanks to the Minnesota Counties Intergovernmental Trust (MCIT), namely Gerd Clabaugh and Eric Nerness, for their input that helped lead to the formation of the AMC Cybersecurity Task Force, and their work to secure cybersecurity insurance for many counties in Minnesota during a time of disruption in that space.

Thanks to the organizations listed below, each of which developed informative, direct, and timely resources to help counties begin and further their cybersecurity journeys:

Minnesota Counties Intergovernmental Trust (MCIT)

Cybersecurity & Infrastructure Security Agency (CISA)

National Association of Counties (NACo)

New York State Association of Counties (NYSAC)

Minnesota Department of Public Safety – Emergency Communication Networks Division (DPS-ECN)

Thanks to the Minnesota Department of Information Technology (MN.IT) for its work toward elevating cyber security awareness and preparedness statewide, especially on behalf of Minnesota in its interaction with the federal offices involved in cyber security.

Finally, thanks to the Minnesota State Cybersecurity Task Force, which is spearheading development of a plan that will hopefully give Minnesota counties access to federal grant funds via the state. AMC looks forward to strong state-county collaboration to modernize our state's cybersecurity posture.

John M. Smith
IT Director
Goodhue County
509 W. 5th St.
Red Wing, MN 55066
Phone (651) 385-3224
Fax (651) 267-4870

To:	Goodhue County Technology Committee
From:	John M. Smith, IT Director
Date:	October 26, 2023
Subject:	Technology Projects in 2023

Projects Completed:

1. Upgrade Pine Island and Wanamingo GCSO Offices
2. Implement Information Security Awareness Program – ARPA Funding
3. Assist Land Use Management with Cloud Based GIS Infrastructure
4. Develop Policies for Website ADA Compliance – Move to Communications
5. Relocation and Remodel of County Board Room
6. Implement Security Incident and Event Management (SIEM) – ARPA Funding
7. Implement Microsoft Office365

Projects in Progress:

1. Migrate to Tyler Property Tax System for Auditor/Treasurer Office
2. Assist Public Works with Lake Byllesby Park Pavilion Security
3. Government Center remodel, phase 1

Projects on Hold:

1. Backup PSAP and Mobile PSAP for GCSO Dispatch
2. Implementation and migration to .gov domain (GoodhueCountyMN.gov)
3. Network Switch Upgrades – Will need to carryover to 2024
4. Multi-Factor Authentication (MFA) for ALL network connections – ARPA Funding
5. Update Support Agreements with County Police Departments – 2024