DAKOTA COUNTY
BOARD OF COMMISSIONERS

RESOLUTION 23C-005

RESOLUTION FOR ESTABLISHING COUNTY CYBER SECURITY POLICIES

WHEREAS, Nebraska Revised Statute §23-106(1) establishes the duty of the county board is to manage the county funds and county business except as otherwise specifically provided; and Nebraska Revised Statute §23-109(1) establishes the county board shall have power to examine and settle all accounts against the county and all accounts concerning the receipts and expenditures of the county; and

WHEREAS, the Dakota County Board of Commissioners wishes to establish a Cyber Security Policy to secure county information and data. Cybercrimes such as phishing and ransomware are a threat to County IT infrastructure and tax-payer funds. The County wishes to protect and secure the confidentiality, integrity and availability of information in cyberspace by establishing the following policies:

1. Acceptable Use of Data Systems Policy
The purpose of this policy is to stipulate the suitable use of computer devices at Dakota County. These rules protect the authorized user and therefore Dakota County also. Inappropriate use exposes the County to risks including virus attacks, compromise of network systems and services, and legal issues.

- **Handbook Employee Conduct Policy:** The County provides email, voicemail, Internet access, telephone service, and computer equipment for use in conducting County business. All such equipment and systems are County property and should be used primarily for business purposes. They may be used for appropriate personal reasons on an occasional basis only during non-working time, unless otherwise permitted under this policy. Because such property and systems are County property, the County has the right to and will monitor the use of such property from time to time. Therefore, no employee should have any expectation of privacy in his/her use of such property or any files, data, or information transmitted with, placed or stored on, or otherwise communicated using such equipment and systems.
  The following will clarify the types of equipment and services contemplated by this policy.
- **Computers**: All data entered on the County's computers is considered the County's property. No employee should knowingly enter false or misleading information in the County's computer system or destroy any data that the County needs to conduct its business. Please realize that, for various reasons, the County will access your equipment. As a result, your computer should not be used for personal business, even during non-working time, if you do not want the County to have access to personal information. Also, unauthorized access to a computer or computer system, or knowingly destroying a computer, computer system, computer software, or computer program, is specifically prohibited. Violators will be prosecuted to the fullest extent allowed by civil or criminal law.
- **Electronic Mail and Voicemail**: Electronic mail and voicemail are to be used primarily for business purposes only. It can be used for appropriate personal reasons only during non-working time. Like your computer, the County will access your email and voicemail when it deems such access necessary. Also, in use of email or voicemail for business purposes, you should be aware that such messages are not entirely confidential. They can be forwarded to others without the original sender's knowledge. Email can be viewed by others who may improperly use a password to breach the security of the system. In addition, disclosure of email messages may be required in lawsuits against the County. As a rule of thumb, nothing should be sent by email if you would not put the information in a formal memo or would not like the information to become public knowledge. Do not use derogatory, offensive, or insulting language in any email or voicemail message. Finally, employees are not to access or view email that is not addressed to them or access or listen to voicemail other than their own. Employees violating this policy will be subject to immediate termination.
- **Use of the Internet**: Use of the Internet is to be limited to business use, except employees may access the Internet for appropriate personal reasons during non-working time. However, pornographic or other offensive sites cannot be viewed at any time. In addition, the County prohibits the downloading or installation of any application software from the Internet onto County computers at any time. This software could contain embedded viruses or be incompatible with our computer operations. Please realize that the County will monitor Internet use.

2. Account Management Policy
The purpose of this policy is to determine a typical process for the creation, administration, use, and removal of accounts that facilitate access to information and technology resources at Dakota County.

- Complete the Riverside Technologies, Inc. (RTI) Employee New Hire Form and Employee Termination Form. See Attachments A (NH) and B (Term)

3. Anti-Virus
This policy was established to assist and prevent attacks on corporate computers, networks, and technology systems from malware and other malicious code. This policy is meant to assist and prevent damage to user applications, data, files, and hardware. Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. Anti-virus software is necessary and a basic necessity for every system.

- RTI has installed FortiEDR which delivers endpoint security with real-time visibility, analysis, protection and remediation. It proactively shrinks the attack surface, prevents malware infection, detects and defuses potential threats in real time.

4. E-Commerce Policy
The frequency of cyber-attacks has been high in recent years. Ecommerce security refers to the measures taken to secure businesses and their customers against cyber threats. This e-commerce policy is to be used as both a suggestion and a summary within the management of the E-Commerce electronic services.

- County Treasurer uses Nebraska Taxes Online Services through MIPS Technology Services Division of Nebraska Association of County Officials (NACO). Certified Payments is an online secure payment system for government entities.
- Clerk of District Court fines can be paid using State of Nebraska .gov online services.

5. E-Mail Policy
Email security may be a term for describing different procedures and techniques for shielding email accounts, content, and communication against unauthorized access, loss, or compromise. Email is usually wont to spread malware, spam, and phishing attacks. Attackers use deceptive messages to entice recipients to spare sensitive information, open attachments, or click on hyperlinks that install malware on the victim's device. Email is additionally a standard entry point for attackers looking to realize an edge in an enterprise network and acquire valuable Dakota County data. Email encryption involves encrypting, or disguising, the content of email messages to guard potentially sensitive information against being read by anyone aside from intended recipients. Email encryption often includes authentication. The purpose of this policy is to determine rules for the utilization of corporate email for sending, receiving, or storing electronic messages.

- Email restrictions – private personal information, such as social security numbers, etc., should not be sent directly through email and if needed should use the option to encrypt the information for transit.
- The County's emails are hosted locally on an exchange server and routed through Office 365 for the purpose of ensuring private information can be encrypted.
- All County emails must be identified using the dakotacounty.ne.gov domain.

6. Hardware and Electronic Media Disposal Policy
The Dakota County-owned surplus hardware, obsolete machines, and any equipment beyond reasonable repair or reuse, including media, are covered by this policy. This policy will establish and define standards, procedures, and restrictions for the disposition of non-leased IT equipment and media in a legal, cost-effective manner.

- Follow Nebraska Statute 23-3115 for all Surplus personal Property; sales; conditions. Both computer and printer hard drives should be removed and destroyed by Commercial Shredder **or** wiped clean by RTI or similar service.
- Emails: follow State Records Retention and Disposition Schedules – emails can be archived by RTI

7. Security Incident Management Policy
This policy defines the need for reporting and responding to incidents associated with Dakota County's information systems and operations. Incident response provides the county with the potential to spot when a security incident occurs.

- Contact the RTI Help Desk [helpdesk@1rti.com] if you see a suspicious email. If you forward the email to the RTI helpdesk, do so by sending as an attachment.

8. Information Technology Purchasing Policy
The reason for this strategy is to characterize norms, methods, and limitations for the acquisition of all IT equipment, programming, PC-related parts, and specialized administrations bought with organization reserves. Acquisition of innovation and specialized administrations for the organization should be supported and facilitated through Riverside Technologies, Inc. (RTI)—the County's IT Management Company.

9. Log Management Policy
Log management is often of great benefit and with proper management, to reinforce security, system performance, resource management, and regulatory compliance will be done by RTI. RTI currently monitors logs for network traffic on the firewall on the local device, wireless AP logs centralized to the Aruba Controller, and their MSSP software agent monitors event viewer logs on all workstations and servers.

10. Network Security and VPN Acceptable Use Policy
The purpose of this policy is to define standards for connecting to Dakota County's network from any host. These standards are designed to attenuate the potential exposure to the County from damages, which can result from unauthorized use of the Dakota County's resources. Damages include the loss of sensitive or confidential data, property, damage to critical Dakota County internal systems, etc. Be aware and employ safe practices for connecting to free and unsecured Wi-Fi. The County provides computer devices, networks, and other electronic information systems to goals, and initiatives. The County grants access to those resources as a privilege and must manage them responsibly to take care of the confidentiality, integrity, and availability of all information assets.

- Only county-approved individuals
- Individuals must use 2-factor authentication
- Devices should only be allowed to connect to their specific county office wireless connection
- Non-county devices should only be allowed on public access wireless connection.

11. Password Policy
The concept of username and passwords has been a fundamental way of protecting our information. This may be one of the first measures regarding cybersecurity. The purpose of this policy is to determine the creation of strong passwords, the protection of these passwords, and therefore the frequency of changing passwords must be followed.

- 8 minimum characters – must use a letter/number/symbol
- Passwords must be changed every 4 months
- Passwords must be securely stored by a Password Manager App

12. Patch Management Policy
Security vulnerabilities are inherent in computing systems and applications. These flaws allow the event and propagation of malicious software, which may disrupt normal business operations, additionally placing the corporate in danger. To effectively mitigate this risk, software "patches" are made available to get rid of a given security vulnerability.

- RTI automatically schedules and deploys to servers and workstations all patches within 2 days of notification from Microsoft.
- All patches run during the evening hours and Computers need to be left on for auto patching. RTI will monitor systems that fail and reach out to the County for follow-through.

13. Cloud Computing Adoption
The purpose of this policy is to make sure that Dakota County can potentially make appropriate cloud adoption decisions and at an equivalent time doesn't use or allow the utilization of inappropriate cloud service practices.

- Consult with RTI so all security measurers can be deployed

14. Server Security Policy
The purpose of this policy is to define standards and restrictions for the bottom configuration of internal server equipment owned and/or operated by or on Dakota County's internal network(s) or related technology resources via any channel.

- Access to servers by outside vendors should be directed to RTI

15. Social Media Acceptable Use Policy
The use of external social media within organizations for business purposes is increasing. The County faces exposure of a particular amount of data that will be visible to friends of friends from social media. While this exposure may be a key mechanism driving value, it also can create an inappropriate conduit for information to pass between personal and business contacts. Tools to determine barriers between personal and personal networks and tools to centrally manage accounts are only starting to emerge. Involvement by the IT Department for security, privacy, and bandwidth concerns is of maximal importance.

- **Handbook Social Media Policy**: We understand that social media can be a fun and rewarding way to share your life and opinions with family, friends, and co-workers around the world. However, use of social media also presents certain risks and carries with it certain responsibilities. To assist you in making responsible decisions about your social media use, we have established the following guidelines for appropriate social media use. This policy applies to all employees who work for the County.
  Guidelines: In the rapidly expanding world of electronic communication, social media can mean many things. Social media includes all means of communicating or posting information or content of any sort on the Internet, including to your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, whether or not associated or affiliated with the County, as well as any other form of electronic communication.
  Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. Keep in mind that any of your conduct that adversely affects your job performance, the performance of your fellow coworkers, or otherwise adversely affects the County's legitimate business interests may result in disciplinary action up to and including termination.
  Know and follow the rules: Carefully read these guidelines, the County's Harassment Policy and Complaint Procedure and Workplace Violence Prevention policy and ensure your postings are consistent with these policies. Inappropriate postings that may include discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including discharge.
  Be respectful: Always be fair and courteous to fellow coworkers, customers, and people who work on behalf of the County. Also, keep in mind that you are more likely to resolve work-related complaints by speaking directly with your co-workers than by posting complaints to a social media outlet. Nevertheless, if you decide to post complaints or criticism, avoid using statements, photographs, video, or audio that reasonably could be viewed as malicious, obscene, and threatening or intimidating, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, sex/gender, disability, religion, age, gender identity, sexual orientation, or any other status protected by law.
  Be honest and accurate: Make sure you are always honest and accurate when posting information or news, and if you make a mistake, correct it quickly. Be open about any previous posts you have altered. Remember that the Internet archives almost everything; therefore, even deleted postings can be searched.
  Post only appropriate and respectful content:

✓ Express only your personal opinions. Never represent yourself as a spokesperson for the County. If the County is a subject of the content you are creating, be clear and open about the fact that you are a County employee and make it clear that your views do not represent those of the County. If you do publish a blog or post online related to the work you do or subjects associated with the employment with the County, make it clear that you are not speaking on behalf of the County. It is best to include a disclaimer such as "The postings on this site are my own and do not necessarily reflect the views of Dakota County."

✓ Do not divulge confidential County information. Examples of confidential information may include information related to pending criminal investigations in the Sheriff's Department and potential prosecution by the County Attorney's Office.

Use of Social Networking Websites on County Equipment, or During Work Hours: Employees are prohibited from using or accessing social networking sites on County equipment. Employees are also prohibited from using their personal equipment for social networking during working hours. Working hours are defined as an employee's scheduled shift, but exclude lunch and other break times. The County reserves the right to monitor employees' website history on County equipment to determine whether employees are complying with this policy.

- Dakota County will work with RTI to control any bandwidth issues.

16. Systems Monitoring and Auditing Policy
System monitoring and auditing are employed to work out if inappropriate actions have occurred within a data system. System monitoring is employed to seem for these actions in real-time while system auditing looks for them after the very fact.

- RTI has installed FortiEDR which delivers endpoint security with real-time visibility, analysis, protection, and remediation. It proactively shrinks the attack surface, prevents malware infection, detects, and defuses potential threats in real time.

17. Vulnerability Assessment
The purpose of this policy is to determine standards for periodic vulnerability assessments. This policy reflects Dakota County's commitment to spot and implement security controls, which can keep risks to data system resources at reasonable and appropriate levels.

- Dakota County will employ an outside vendor once or twice a year to conduct a risk-based assessment of the County and it's managed IT provider--RTI.

18. Website Operation Policy
The purpose of this policy is to determine guidelines with reference to communication and updates of Dakota County's public-facing website. Protecting the knowledge on and within the corporate website, with equivalent safety and confidentiality standards utilized within the transaction of all the corporate business, is significant to Dakota County's success.

- MIPS webmaster contact info is: webmaster@nebraskacounties.org

19. Workstation Configuration Security Policy
The purpose of this policy is to reinforce security and quality operating status for workstations utilized at the County. IT resources are to utilize these guidelines when deploying all new workstation equipment. Workstation users are expected to take care of these guidelines and to figure collaboratively with IT resources to take care of the rules that are deployed.

- RTI manages each County workstation and will conduct Quarterly reviews with management to define rules intended to reduce the risk of data loss/exposure through workstations.

20. Firewall
A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the Internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence, firewalls play an important role in detecting malware.

- RTI has installed FortiEDR which delivers endpoint security with real-time visibility, analysis, protection, and remediation. It proactively shrinks the attack surface, prevents malware infection, detects, and defuses potential threats in real time.

21. Malware scanner
This is software that sometimes scans all the files and documents present within the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are samples of malicious software that are often grouped together and mentioned as malware.

- FortiEDR manages this on a bi-weekly basis.

THEREFORE, BE IT RESOLVED, that the Dakota County Board of Commissioners hereby approves said cyber security policy.

Dated this 6th day of February, 2023.

ATTEST:

Cherie Conley

Cherie Conley, County Clerk

DAKOTA COUNTY CLERK OF DAKOTA COUNTY NEBRASKA

Robert J. Giese, Board Chair