

AD HOC TRANSITION COMMITTEE MINUTES

March 19, 2014, Room A260 1:00 p.m.

The meeting was called to order by Chairman Miller at 1:00 p.m.

Roll call: Johnson, Stuchlak and Miller present. Excused, West and Bays. Also present Wagner, Kaye, McGhee, Wollin and Kotlowski.

The meeting was properly noticed.

Motioned by Stuchlak/Johnson to approve the agenda. Motion to approved carried by unanimous voice vote.

Motioned by Stuchlak/Johnson to approve the minutes from March 6, 2014. Motion carried by unanimous voice vote.

Motioned by Stuchlak/Johnson to deviate to 6K, A – J then return to 6A. Motion to deviate carried by unanimous voice vote.

A. Equipment & Data Security

1.01 Equipment Security.

- a. Hardware (computers, printers, etc.) cannot be relocated without prior approval from MIS. Purpose is to ensure an accurate inventory and to help prevent equipment from being unnecessarily damaged.
- b. Users are not permitted to install new or replacement hardware.
- c. Personal hardware – Personal electronic hardware brought from home may not be connected or installed onto any county computer or onto the county network. Examples are modems, digital cameras, PDA's, printers, Blackberries, tablets, smartphones etc.

1.02 Data Security.

- a. Personal computer equipment cannot be connected to the Adams County Network in any way unless approved by the MIS Department.
- b. Computer modems are only permitted to be connected to a phone line when the modem is used as a direct connection to a state network for relaying data to that network. Dial up internet connections are not permitted on computers connected to the Adams County infrastructure and are a security violation.
- c. Users are not to remove or disable any administrative, security, or virus scanning software from their computer.
- d. Software programs cannot be downloaded from the internet or brought to work by a user and installed on any computer.
- e. Computer monitors that will display PHI (Personal Health Information) should not be viewable from outside the employees' office or workstation. Each PC should be locked into screensaver mode or logged off before a worker leaves their office.
- f. All Computers are required to have an idle PC lockout after 15 minutes of idle time. All users are encouraged to log off or lock (Ctrl+Alt+Del) the computer system before leaving their computer unattended. MIS will reserve the right to log off the computer after 1 hour of inactivity for network security purposes and to allow maintenance to be performed on the computers during off hours.

1.03 Password Security.

- a. All user passwords will be require to be changed every 90 days. Users will be prompted to change their passwords. Users can also press CTRL+ALT+DEL and choose "Change Password" if they would like to change it prior to the 90 day limit.
- b. Passwords are required to be at least 7 characters in length. Passwords should contain a combination of numbers, letters, and special characters.
- c. Users will not be allowed to use a previous password when their password expires.

- d. Passwords must not be accessible to any other users. The password must be memorized, not written. Each user is solely responsible for all computer transactions, such as internet use, emails and file access, which take place using their username & password. Users are prohibited from sharing access to their computer while logged on.
- e. Users must notify MIS immediately if they feel their password or account has been compromised.
- f. Contact the MIS helpdesk at #567 if a password is forgotten. MIS can reset passwords as needed.
- g. Network, Internet and Email access are associated with the user's logon and password. If the user is not granted permission by the department to use these resources, their profiles will restrict them from doing so.
- h. MIS may ask a user for his or her password to install and troubleshoot hardware and software. MIS will maintain the confidentiality of the password or, if requested, can reset the password for the user to change at next logon. MIS may also reset the password to troubleshoot a PC. If this is the case, MIS will prompt the user to change the password at next logon. Users can also change their own network password at any time by pressing Ctrl+Alt+Del and clicking on the "Change Password" button.
- i. Users are prohibited from sharing their passwords with non-MIS Staff.

1.04 File Security.

- a. Based on the information from the IT Employee Access Change Form, MIS assigns folder and file access permissions to specific users and groups of all directories to control which user has what level of file access on the network.
- b. Users are responsible to manage their files by storing them in the correct location based on security requirements.
- c. Removable disk storage media – Each employee is responsible for the maintenance and security of the data they store onto removable storage media. PHI (Personal Health Information) must be consistent with the Adams County HIPPA Policy. ~~Users must ensure the devices are password protected if they contain county data. Users must also password protect any confidential data should these devices be lost and fall into a person's hands who is not authorized to see the information.~~
- d. Workstation **Security**. The County will implement policies and procedures to keep end point systems (defined as desktops, laptops, palm computers and tablets) physically secure and accessed only by authorized users. Special care must be taken to protect information that is considered particularly sensitive. Any variation from these procedures must be approved in advance.
- e. Physical safeguards for end point equipment will be provided so as to prevent public access.
- f. For all cases other than computers designated for public use, security will be provided by restricting and controlling physical access to the offices and desktop systems and by properly positioning and protecting systems such that information cannot easily be read or obtained.
- g. Monitors should generally be kept from the plain view of anyone who does not have the appropriate access or clearance to information that may be displayed.
- h. Keyboard, mouse, and other components should be kept far enough away from the public, so they cannot be tampered with, or stolen.
- i. Printers should also be kept in protected areas to keep sensitive information from being disclosed inappropriately.
- j. Printer materials from any source should be kept secure and away from viewing and out of public reach.

1.05 Software.

- a. Personally owned software brought from home may not be connected or installed onto any county computer.
- b. Employee Responsibilities:
- c. Employees shall not knowingly introduce a computer virus into company computers.
- d. Employee's shall not disable or uninstall security, antivirus or monitoring software from any county owned equipment
- e. Employees shall not load diskettes, CD's, DVD's, USB Jump Drives and other portable media of unknown

origin that is network attached.

- f. Incoming diskettes, CD's, DVD's, USB Jump drives, and other portable media shall be scanned for viruses before they are read (Real time monitor checks this for employee).
- g. Any associate who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the MIS Helpdesk at 339-4567 or ext. 567.
- h. All software acquired for or on behalf of Adams County or developed by Adams County employees or contract personnel on behalf of the County is and shall be deemed county property. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements. County software may not be duplicated.
- i. Licensing - Unless otherwise provided in the applicable license, notice contract, or agreement, any duplication of copyrighted software, except for backup and archival purposes, may be in violation of federal and state law. In addition to violating such laws, unauthorized duplication of software is a violation of this Software/Hardware Policy.

1.06 Network. File Management, Backup & Retention

- a. Users are encouraged to manage their files in a professional manner by deleting unnecessary, outdated, and duplicated files.
- b. The MIS department reserves the right to limit user storage space and to setup auto-archiving of aged data should the user not comply in managing their files.
- c. Users are not permitted to store music files or video files for personal use on county equipment. Storage of personal media files could implicate the county in copy write infringement.
- d. Peer to Peer (P2P) networking is prohibited on the County network unless authorized and configured by the MIS Department.
- e. Changes to user phone settings must be requested in writing.
- f. Voice mail is available to users and must be approved by the Department Head using the Employee Access Change Form.
- g. Phones and fax machines cannot be moved before contacting the MIS Department for proper configuration on the associated ports or jacks.
- h. Internal phone extensions are 3 digit numbers and cannot be dialed from outside of the Courthouse. Extensions starting with the number 2, 3 or 5 have a corresponding external number: 339-4xxx, xxx being the extension number.

B. General IT Information Management

1.01 Introduction. Computers and related equipment and software play a rapidly increasing role in County Government. This Computer Policy shall govern the acquisition and use of computers and computer-related equipment (including software, printers, monitors, speakers, laptops computers, facsimile, modems, Internet access, and email) throughout the County including all its Departments and sub-units. The enclosed policies and directives have been established to:

- A. Protect this investment.
- B. Safeguard the information contained within these systems.
- C. Reduce business and legal risk.

1.02 Policies may be based on a combination of law, administrative policy and commonly accepted business practices; and will be determined based on the best interests of Adams County Government and its constituents. This policy will be reviewed at least annually, or as often as may be required to respond to changes in laws, technology or other requirements.

- A. Site surveys should be conducted: semi-annually by the Department Head and a report of any infraction shall be reported to Technology Steering Committee.
- B. It is the responsibility of Adams County Government and Department Heads to determine the access and security requirements for each building and office area.
- C. There will be some cases in which end point equipment will be accessible to the general public. In general, the following rules along with the Public Access Policy will apply.

- i. The equipment will be in an office suite or building, which can be locked or secured after normal business hours.
 - ii. The equipment will be monitored to ensure that it is not removed or intentionally damaged while accessible to the public.
 - iii. The equipment will be technically locked down so that a member of the public cannot access our internal secured networks.
- D. Adams County will use standards that support workstation security. These include, but are not limited to:
- i. Utilization of Windows XP or Vista operating systems, appropriately patched.
 - ii. Utilization of a locked down configuration – that each user will not have local administrator rights on their workstation.
 - iii. Utilization of Windows automatic screen saver function that is password protected. Such screen savers will automatically activate after 15 minutes of inactivity.
 - iv. Users or departments will take no action that disables the use or prolongs the time frame of such security measures.
 - v. The County considers workstations as a sensitive item

**ACCESS TO COUNTY NETWORK
SECTION – 2**

2.01 Requirements for New & Departing Employees.

Forms are required for:

- A. New & Transferred Employees Network Access—Each Department is required to notify the MIS Department at least 1 week in advance of new employees hired. Access Change Form must be completed, signed by the Department Head, and submitted to MIS by this time, when possible. The Access Change Form defines permitted computer programs and data access.
- B. Departing Employees—Each Department is required to give the MIS Department at least 1 weeks notice of employees departing employment at Adams County. An Access Change Form must be completed and signed by the Department Head by this time. The Access Change Form defines to MIS when the user profiles should be disabled and/or deleted and how the user's data files and old email should be handled.
- C. Departments may have "generic" profiles for temporary positions such as an LTE or intern. However, this profile can only be assigned to one person at a time and the password will need to be changed prior to a new person using the profile. When the profile is not used, MIS will disable it.
- D. Each department should request network access for their external users that may need to access their computer systems, such as contractors, via Access Change Form.

C. Privacy & Monitoring/Resolution;

1.01 Monitoring

- 1. All Adams County resources, including but not limited to, computers, Internet access, e-mail and voice mail may be monitored by the County. At any time and without prior notice, Adams County maintains and intends to exercise the right to examine any systems and inspect and review any and all data recorded in these systems. Any information stored on a computer, whether the information is contained on a hard drive, computer disk or in any other manner may be subject to review by the County. This examination helps ensure compliance with internal policies and the law. It supports the performance of internal investigations and assists the management of information systems.
- 2. Adams County has employed monitoring software to check on the use and content of the Internet and e-mail to ensure that there are no serious breaches of this policy. The County specifically reserves the right for authorized personnel to access, retrieve, read any communication that is created on, received through, or sent via the e-mail system, to assure compliance with all County policies. Such monitoring may be initiated randomly or may be

initiated upon a complaint upon reasonable suspicion of misuse of internet or email by an employee and shall be used for legitimate purposes only.

PRIVACY SECTION - 2

2.01 Privacy

Adams County reserves and intends to exercise the right to review, audit, access and disclose any and all files created on any county computer.

- A. Employees shall have no expectation of personal privacy when using computers, including all e-mail activity and internet use.
- B. Passwords are not an indicator of personal privacy from employer monitoring.
- C. Adams County's failure to monitor in particular situations is not a waiver of the Counties right to monitor in the future.
- D. Monitoring - All Adams County resources, including but not limited to, computers, Internet access, e-mail and voice mail.

Incidental and occasional personal use of the Internet or the corporate e-mail system is permitted, subject to the restrictions contained in this policy or any related departmental policy. Any personal use of internet or e-mail is expected to be on the employee's own time and is not to interfere with the person's job responsibilities. Personal use of these systems must not detrimentally affect the job responsibilities of other employees, disrupt the system and/or harm the County's reputation.

D. Security

1.01 Introduction. Information security is not the sole function of any department, group, or agency. Rather it is a result of the combined efforts of leadership to provide guidance and state intent, a committee to create policies, technical staff to implement the technical structures that support the policies, managers and supervisors to train, implement, and ensure compliance with the policies, and the personnel system to provide enforcement and sanctions when policies are broken.

1.02 Physical Security. It shall be the policy of Adams County that all data centers and closets are secured, restricted areas. Access shall be granted to only those individuals who have a mission essential business need and who have been appropriately cleared. County data centers contain data, which is sensitive, personal in nature and in some cases protected by law. Data centers are not common workspaces. Traffic in the data centers shall be kept to a minimum. Unaccompanied access to data centers and closets shall require signing of the County Non Disclosure Agreement.

1.03 Incident Response and Reporting. Adams County will adhere to a standardized procedure of responding to security incidents, investigating these events, documenting the results of those investigations and taking appropriate action to meet operational and legal requirements for addressing the incident. The county shall maintain preventative measures to avoid any reasonably anticipated events that would compromise the confidentiality, integrity or availability of data stored on the County network or County owned devices. It is also the intent of this policy that each investigation contains recommendations and courses of action that will lessen the likelihood of a recurrence whenever possible. This applies to all actual or suspected security incidents on Adams County networks, including attacks emanating from outside the County, business partner connections, wireless and remote access, or the theft or unauthorized removal of media, data, storage devices, disks or CDs. This policy applies to all county employees, elected officials, boards, committee and commission members who have access to County systems, interns, contractors, affiliated or tenant agencies, business partners and volunteers.

~~A. Description and Definitions of Incidents~~

- ~~1. Denial of Service: DoS attacks are those incidents which cause network or information resources to abnormally terminate operations, degrade operation or be disrupted or interdicted to the point where they are not efficiently performing their intended function. This can be caused by a targeted~~

attack from one or more internal or external sources, a server crash or network failure either by intentional attack or natural occurrences, or a denial of physical access to a facility or device. Such an event could affect critical systems used throughout the County and would need to be addressed immediately and investigated.

2. ~~Malicious code: Any worms, Trojan horses, root kits, or viruses brought into the county network intentionally or unintentionally have the potential to attack and destroy data quickly, or to compromise the confidentiality and integrity of information. Such an event would require immediate attention.~~
3. ~~Unauthorized access: Anyone gaining access without authorization to the county network or county owned media, devices, or servers would be classified as a violation of policy and a security incident. This incident would require immediate attention and coordination between multiple departments.~~
4. ~~Inappropriate usage: The accesses of systems, networks or data without full compliance of all policies.~~
5. ~~Mixed or blended attack: An incident would be comprised of multiple categories or incidents. The relative severity of a blended attack would be based on the information gathered at the time of the attack or detection.~~

~~B. Incident response and reporting procedures~~

1. ~~Preparation and prevention: the process of creating a policy, severity index and reporting structure for incidents, and creating a security posture which may prevent incidents from occurring or reoccurring.~~
2. ~~Detection and analysis: The steps involved in identifying an incident, providing immediate notification to appropriate parties, analyzing the available information, creating an action plan, gathering data and or evidence and determining extent of access or damage.~~
3. ~~Containment, eradication and recovery: the processes involved with stopping the spread of the incident or problems, cleaning affected systems, recovering data, involving law enforcement agencies (if appropriate) finalizing the collection of logs and data and returning systems or networks to a fully operation condition.~~
4. ~~Post Incident activities: Determining the root cause, creating final reports, notifying affected individuals, complying with all legal requirements for notifications and documentation, determining corrective actions and ensuring that those corrective actions become part of the preparation and prevention process are all requirements.~~

~~C. Incident response and reporting procedures~~

1. ~~Preparation and prevention phase: A notification system will be designated so that employees may report security incidents through a variety of methods, to include electronic mail, in writing, by telephone or in person confidentiality will be maintained to the greatest extent possible. These methods will be included in the new employee orientation training.~~
2. ~~Technical measures will be taken, consistent with budgeting and personnel levels to monitor and prevent security events as are reasonably appropriate.~~

~~D. A. Detection and analysis~~

1. ~~The county will adhere to a policy of flexible response, such that minor events can be handled and cleared quickly, with minimal involvement, but the more serious matters involve more personnel. Depending on the severity, a determination will be made as to who needs to actively participate in the investigation.~~
2. ~~(ii) Staff will be included as necessary to assess systems or networks, complete any required investigation items in the time frame allotted. In the event that specialized expertise is required or criminal activity may be involved, contractor or law enforcement resources may be called upon possibly including the FBI and Department of Homeland Security.~~
3. ~~It shall be the policy of Adams County that there will be no punishment or adverse action for the good faith reporting of security issues, problems or incidents.~~

~~E. B. Containment, eradication and recovery~~

1. ~~Priority will go to identifying the scope of the incident or attack and containing its spread.~~

2. Every attempt will be made to retain and collect evidence, which could be useful to the investigation.
3. Systems beyond the initial scope of the report may need to be examined to determine the number of devices involved.
4. No system will be left on line until it is determined that it is not harmful to networks or other systems.
5. Recovery will proceed as quickly as possible, without compromising security or unnecessarily exposing other systems to compromise or damage.

F. Post-incident activities

1. ~~6.~~ An incident report will be ~~created.~~ started in TrackIT, ~~creating a diary of the events as they transpire.~~ All documents, reports, logs, written summaries of interviews, files, etc. will become part of the official record of the investigation. This information will be protected from public disclosure as permissible by law.
2. ~~7.~~ Reports will include whenever possible, the proximate causes and recommended corrective actions.

E. Statement & Responsibilities/Resolution;

STATEMENTS OF RESPONSIBILITY

SECTION - 1

1.01 Introduction. General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities. Access to information is a public trust and is to be protected with all prudence and diligence. The information systems we utilize are mission-critical devices that we depend on to conduct the business of the County and to support our citizens and residents as well as other government agencies.

1.02 Department Head. Department Heads are responsible for determining who will be allowed to access their information, consistent with polices, applicable laws and regulations governing access. The Department Head may delegate this authority to one other person; however the final responsibility for establishing clear guidance for their data, and enforcing security policy lies with the Department Head.

1.03 Management Information System. MIS houses, administers and operates all servers, infrastructure and security equipment for Adams County agencies, unless special exceptions are granted, by the MIS Department with consultation with Corporation Counsel if need be, the MIS Department is the custodian of the County's information resources and implements the policies set forth in this document. MIS acts on behalf of Adams County Government and Department/Division Heads to secure information, applications, systems and networks, to provide authorized access to approve personnel and to monitor, detect, investigate and report on actual or suspected security breeches or incidents.

1.04 End User/Employees. Employees of Adams County, and others accessing county information or computer services, play a key role in maintaining the integrity and security of all of our automated systems. Each user of automated services is responsible to understand these rules and guidelines, to abide by them as well as to identify and report issues and problems.

F. Support/Resolution;

SECTION 6 – SUPPORT

~~6.01 General.~~ The MIS Helpdesk is available Monday through Thursday 8am to 5pm and Friday 8am to 4:30pm each normal work day by calling extension 567 or 339-4567. Should the helpdesk not answer, they are either on a call or had

to step away momentarily. Please leave a message and you will receive a call back usually within 30 minutes. The MIS department also has someone "On Call" 24 hours a day 7 days per week & 365 days a year to resolve critical issues that absolutely cannot wait until the next work day. The 911 dispatchers can page MIS for after hour emergencies. Please note that poor planning does not constitute an emergency.

6.02 Levels of Support.

- ~~A. Level 1~~ End users are expected to check obvious things such as electrical power, cable connections, etc. A common solution is to reboot (or restart) the computers.
- ~~B. Level 2~~ The MIS Helpdesk can be contacted by calling extension 567 or 339-4567. Whoever answers the phone will open a new problem ticket and verify the required information, and may work with the user over the phone to correct the issue.
- ~~C. Level 3~~ If the issue cannot be resolved over the phone the MIS Department will work to resolve this ticket either on-site or remotely. If the ticket cannot be completed in a timely fashion, the MIS staff may contract with an outside contractor to do the work.

F. Hardware, Phone System/Resolution;

1.01 General Statements.

- A.** All Adams County issued equipment (to include laptops, cell phones, PDAs, etc.) and all data generated, received or stored on such equipment are property of Adams County.
- B.** Software, hardware, and network systems are intended to be used for business purposes only to increase the quality and timeliness of services provided to the taxpayers of Adams County.
- C.** Purchasing - All purchasing of Adams County hardware and software shall be centralized with the Management Information Systems department to ensure that all hardware and software conform to county software standards, are purchased at the best possible price, and inventoried.
- D.** Disposal of old Hardware and Software - MIS will make the final determination as to the disposition of computer equipment.
- E.** Exceptions to this policy must be approved by the Administrative and Finance Committee. A list of exceptions to the policy shall be maintained by the MIS department. Exceptions may be granted by MIS department prior to committee approval, but must be reported back at the next regularly scheduled meeting.

1.02 Hardware. All hardware equipment acquired must be approved by the MIS Department. All hardware must be used in compliance with applicable licenses, notices, contracts, and agreements.

- A.** Computers & Monitors – All computers have red asset tags associated with them for inventory & naming purposes. Computers are to be used for county business and it is important users understand anything stored or transmitted via a County owned computer is owned by the County. MIS will make every effort to keep computers up to date.
- B.** Users are not allowed to move equipment without the authorization of the MIS Department prior to the move.
- C.** Cell phones UMTS (universal mobile telecommunications systems) and CDMA (code division multiple access) service devices. Strike lines 1202-1205 of employee manual. Modify resolution to incorporate.
 - ~~1.~~ ~~CDMA (code division multiple access) laptop cards for Cellular internet access~~ All devices must be approved by a users Department Head and the Administrative Coordinator/Director of Finance before MIS is notified to make the purchase.
 - 2.** Users are not permitted to access the internet through their cell phone unless approved by their Department Head and department's home committee.
 - 3.** Adams County strongly discourages the use of a county cell phone while driving a vehicle.
 - 4.** Please see the County cell phone policy for more information.
- D.** Printers and Copiers Managed Print Services

- ~~1. Departmental Printing—Although departmental printing is not as convenient for the worker, network printing centralizes larger and faster printers in designated areas for users to print to. By doing this, the county saves thousands of dollars each year because:~~
- ~~2. Small printers do not have to be purchased for every PC.~~
- ~~3. Fewer printers have to be maintained by the MIS Dept.~~
- ~~4. Fewer supplies need to be ordered or kept on hand.~~

All County Departments will participate in the County Manage Print Services contract. All printers and copiers will be enrolled.

- ~~E. Copy Machines—Copy machines should also be used for printing and network cards should be leased or purchased with the copier.~~
- ~~F. Modems—Modems are permitted only on computers that are used for direct billing as necessary to communicate with State and Federal Agencies for billing.~~
- G. The MIS Department maintains a listing of authorized & licensed software programs. This list is comprised based on the following.
 1. Whether the software is required for a department to do their job
 2. Interoperability with other software's owned by the county and the State of Wisconsin.
 3. Software cannot duplicate the functionality of other software.
 4. Simplicity of use and maintaining.
 5. Cost
 6. Hardware requirements
 7. Software conflicts
 8. Other miscellaneous factors
- H. Virus Scanning - The MIS Department will make every effort to prevent viruses from infiltrating County computer systems. Each PC has virus scanning software installed and configured to check for viruses real-time. Also, a virus scanner is setup to check all incoming and outgoing messages before they arrive or leave the mail server.
 1. MIS Responsibilities:
 - a. Install and maintain appropriate antivirus and anti-spyware software on all computers and servers.
 - b. Respond to all spyware & virus attacks, destroy any detected, and document each incident.
- ~~I. Network Drives: When users logon to the network, MIS scripts each users drive mappings. The standard drive mappings listed below are backed up each night, Monday through Friday:~~
 - ~~1. T:\ = This folder is used to store data that is common to all users of the county.~~
 - ~~2. H:\ = This drive is used to store users work files that no one except the user has access to. This drive should be used to store confidential data if such storage is necessary.~~
 - ~~3. S:\ = Each department has an S drive, this is place for everyone in that department to share data files. Only members of each department can access the department folders unless the Department Head requests in writing to allow another user access.~~
 - ~~4. MIS may also map other drives for specific departmental or administrative purposes.~~
 - ~~5. MIS Department staff has access to all drives on the network to allow for system access to maintain file integrity and security, manage backup sets, and be able to restore erroneously deleted files or data.~~
- ~~J. Adams County uses several systems to backup the hardware and data stored on county owned and maintained systems. Data backups are not meant as archives for records, backup software is a tool used by the MIS Department to protect the integrity of the County data:~~
 - ~~1. Backup of Data is done on the following schedule and kept for the designated times:~~
 - ~~2. Daily backup tapes are kept for 1 week.~~
 - ~~3. Weekly backup tapes are kept for 1 month~~
 - ~~4. Monthly backup tapes are kept 5 months~~
 - ~~5. Year end backup tapes are kept for 2 years.~~
 - ~~6. Backup sets run monthly and yearly are kept off site in a fire safe area or vault.~~
 - ~~7. AS400 and Linux backups run separately but follow the same procedure.~~

~~8. Backups of particular data may be requested, such as a End of Year Financial, those will be given to the requesting department and will be maintained and secured by them. The requesting department will be charged for the necessary media.~~

1.03 Phone System. The MIS Department shall be responsible and on call to support the County's phone system.

1.04 System Maintenance.

- A. All scheduled computer or network maintenance which will impact production shall be done after normal work hours whenever possible.
- B. MIS shall make every effort to notify all users via email of any scheduled computer or network maintenance at least 24 hours in advance.
- ~~C. All "Network Maintenance Notifications" (NMN) maintenance notifications shall be titled "NMN" followed by a description.~~
- ~~D. Computers for non 24X7 departments will be shut down each night.~~

G. Definitions & Terms/Resolution;

1.01 Definition of Terms.

- A. Department Head: refers to the Director or Manager of a department or agency, or the department's designee.
- B. Internet: - refers to an "External" network with many web servers containing web pages used to display information to the public.
- C. County Web Page - refers to the URL co.adams.wi.gov for the purpose of providing county related information to the public.
- D. Filtering - To filter and block certain items from the Internet based on URL address, category, user, port, protocol, attachments and other criteria.
- E. Malicious Code - Computer viruses or other programs introduced purposely to disrupt, destroy or damage County information technology.
- F. Internet Service Provider (ISP) - Internet provider selected for use by Adams County to provide Internet access.
- G. Spam - Unsolicited e-mail that is received.
- H. Web Based E-mail - Refers to Internet web sites that offer free browser based e-mail in an effort to lure users onto their site to promote advertisements and services.
 - i. E-mail filtering is also used to detect certain phrases that may also be prevented from incoming and outgoing messages. The MIS Department is responsible for filtering and e-mail system reporting.
 - ii. Virus Protection - The County Email system has virus detection software loaded on the server to check all incoming and outgoing messages on the server for email viruses. This software is updated daily to keep up to date with new viruses.
 - iii. Spam Filtering - Adams County has spam filtering software to prevent thousands of junk (spam) email messages from being sent to employees inboxes.
 - iv. (vii) External E-Mail Accounts - Other Internet providers such as State agency or university accounts in lieu of a County account may be used. However, if the internet and/or email is accessed using the County's ISP, the user will need to adhere to this policy. Licensing, maintenance and compliance to any records retention policies are the responsibility of the providing agency.
 - v. (viii) E-mail Retention - The legal custodian and each user are responsible for maintaining public record e-mail messages and attachments. To that end the MIS Department has implemented email archiving. All incoming and outgoing email messages (whether determined to be a public record according to Sec. 19.32 to Sec.

19.39, Wis. Stats. Wisconsin Public Record Law or not) will be archived for a period of 7 years and then will be destroyed. Users may print out and file public record e-mail messages and attachments for email that has to be kept indefinitely.

- vi. E-mail Records Request Process: All questions or requests made to Adams County for viewing public record e-mail messages should be sent directly to the records custodian. Any questions from users regarding whether or not an a message should be released under the record retention policy should be directed to the Corporation Counsel. The request will then be processed by records custodian.

1.02 Ticket Priority Definitions.

- ~~A. **Critical**—Every effort must be made to resolve or down grade the ticket within 4 hours. Critical status will usually mean that an item effects daily operations for more than a single user or system.~~
- ~~B. **High**—Every effort must be made to resolve or down grade the ticket within 24 hours. High status usually means that an item is more than an inconvenience but does not stop normal day to day functions for an office~~
- ~~C. **Medium**—Every effort must be made to resolve or down grade the ticket within one (1) week. Medium status normally means that an item is an inconvenience to the user or users. However other options are available and can be used.~~
- ~~D. **Low**—Every effort must be made to resolve or down grade the ticket prior to the tickets due date.~~
- ~~E. **Pending**—Is a ticket status that allows MIS to put the ticket on hold until more required information is received from the user who submitted the ticket.~~

1.03 Maintenance.

- ~~E. All scheduled computer or network maintenance which will impact production shall be done after normal work hours whenever possible.~~
- ~~F. MIS shall make every effort to notify all users via email of any scheduled computer or network maintenance at least 24 hours in advance.~~
- ~~G. All "Network Maintenance Notifications" (NMN) maintenance notifications shall be titled "NMN" followed by a description.~~
- ~~H. Computers for non 24X7 departments will be shut down each night. (move to Hardware & Phone System Policy)~~

H. Budget Process/Resolution;

1.01 The MIS Department will compile a single budget for all technology and services covered under this policy for Adams County. Each department will provide to the MIS department on or before June 15th a MIS Budget Planning form.

1.02 Budget Approval Process.

- A.** June 15th all Departments requests for hardware, software or services will be turned into the MIS department.
 1. MIS begins meeting with Departments to discuss requests to confirm compatibility and need.
- B.** July 15th MIS begins to incorporate all Departmental Technology Requests into the final Master MIS budget.
- C.** August Administrative and Finance Meeting(s): MIS begins meetings to discuss budget with home committee and get approval.
- D.** November – County Board Meets for final budget approval
- E.** January – Expenditures begin for budgeted items.

Motioned by Stuchlak/Johnson to approve Technology Policies K, a, b,c,d,e,f,g,h,i and j as amended and forward with resolutions on to county board. Motion carried by unanimous voice vote.

Discuss and/or act on:

a. Open Records-Resolution

Open Records. Public policy favors providing members of the public with access to information and records of governmental activities. The policy is based on the idea that all persons are entitled to the greatest possible information regarding the government and the official acts of those Officers and employees who represent them. Confidentiality is actually an exception to the Open Records and Open Meetings Law.

Each Elected Official, Appointed Officer and/or individual Department Head, or any local public official per Wis. Statutes 19.32 (1dm) is the legal custodian of his/her records and the records of the office.

~~The Department or Committee Member preparing the agenda shall notice the agenda of a meeting at least twenty four (24) hours in advance of the meeting for the public, all members of the news media who have requested notice, and the official newspaper. As a general rule it is advised by the Attorney General that it should be noticed in three different locations. The agenda shall include time, date, place of the meeting, and subject matter. If there is an anticipated closed session it must be noticed as such in accordance with Wisconsin Statutes. In an emergency situation, a meeting may be called without twenty four (24) hours notice, emergency meetings do require at least two (2) hours notice of the meeting.~~

~~The Department or Committee Member preparing the minutes is responsible for submitting a hard copy of the unapproved meeting minutes with associated handouts/attachments to the County Clerk within ten (10) working days after the meeting.~~

b. Contract, Lease, Titles;

All original contracts, titles and/or leases shall be reviewed and initialed by the Corporation Counsel and Administrative Coordinator/Director of Finance ~~All contracts and/or leases are~~ and signed by the Department Head. ~~after review of the Corporation Counsel.~~

Any contract or lease that funding is not available for shall be forwarded by a resolution to the County Board.

A **hard** copy of all **original** signed contracts, titles and leases shall be provided to the County Clerk by the Department Head within five (5) working days and shall be held in the name of "Adams County Government" unless otherwise stated by law.

It is the responsibility of the Department Head to follow all contract and lease regulations to ensure all monies are received and paid on time. If funds are received, it is the Department Head's responsibility to deposit the funds with the County Treasurer.

c. Exit interview/Resolution;

Exit Interview. The Exit Interview is used to gain insight into the effectiveness of County personnel and managerial practices, to determine where policies and procedures are in need of review or revision, and where supervisory or managerial practices need modification or improvement. Employees are requested to complete the Exit Interview Form and return it to the Personnel Director. A summary of comments will be provided to the Department Head and Home Committee.

d. Recognition/Resolution

~~**Recognition.** Recognition for years of service will be given to the members of the County Board, Committees, Boards, Commissions and all County employees and volunteers as follows:~~

~~A. A certificate for every five (5) years of continuous service.~~

~~B. A plaque for twenty five (25) years of service.~~

~~C. A clock for those who retire or leave (excluding disciplinary termination) after ten (10) continuous years or more of service along with a resolution thanking the employee for all their years of service.~~

~~All recognition will be given at the January County Board meeting for all items with the exception of the clock, which will be given at the time of termination and the plaque, which will be given at the County Board meeting in the quarter the employee attains twenty five (25) years of service. Strike completely and look at other options in the future.~~

e. Daylight Saving Time;

Daylight Savings Time. Employees who are required to work during the change of Daylight Savings Time shall be paid for the actual hours worked.

f. Travel Time;

Reimbursement for Travel Time. Federal Law applies to compensation for travel time required of FLSA non-exempt employees. For same-day out of town travel, any FLSA non-exempt employee who is required to travel during hours that are in addition to the normal workday shall be paid overtime for those hours. If the travel is overnight, then a FLSA non-exempt employee is eligible for overtime for hours that are in addition to the normal workday. only if he drives an automobile to the conference. Department Heads shall contact the Personnel Director prior to any overtime travel pay. In no instance shall an employee be paid to travel to the employer's work site if it is the first stop of the day. In this case the employee begins being paid once the employee arrives at work.

g. In-line structure;

<ul style="list-style-type: none">• Admin Coordinator• Corporation Counsel• Personnel Director <p>-Provide data, make recommendations, insure policies are consistently followed -No decision making authority -Decision making authority ONLY in their departments</p>

COUNTY BOARD -Ultimate Decision-makers for entire county
--

OVERSIGHT COMMITTEE -Appropriate coms.(s) make decisions -May involve multiple committees (i.e. budget matters Oversight com. Finance com)

<ul style="list-style-type: none">• Admin Coordinator• Corporation Counsel• Personnel Director <p>-Provide data, make recommendations, insure policies are consistently followed -No decision making authority -Decision making authority ONLY in their</p>

DEPARTMENT HEAD -Provide data, make recommendation -Decision-making authority for department operations
--

DEPARTMENT STAFF -Implement plan of operations
--

h. Purchasing Policy;

General. Adams County uses a decentralized purchasing system. This type of system authorizes each department to purchase their own goods and services within County guidelines.

There are currently no purchasing thresholds established other than the ones established by §59.52(29) and §66.091, Wisconsin Stats., regarding public works. Purchasing thresholds are established by the annually approved County Budget as administered by the respective Department Head and as overseen by the respective Oversight Committee(s).

Purchasing Rules & Regulations.

- A. Competitive bidding is not required for contract unless there exists a specific legal requirement that bidding proposals be advertised. Except where required by statute, the County is free to negotiate contracts, as it deems necessary.
- B. Adams County follows §59.52(29) and §66.0901, Wisconsin Stats., for public works contracting and bidding and shall comply with all prevailing wage requirements.
- C. Professional services are not subject to the bidding statutes on the theory that public bodies should be free to judge the qualifications of those who are to perform such services.
- D. Purchases defined as "equipment" are not a supply or material, and are therefore not subject to the bidding statutes.
- E. All bids are final as opened at the Oversight Committee level.
- F. All bids shall be awarded by the Oversight Committee.

i. Response Time;

Response Time. In order to respond to emergency and service needs, employees may be required as part of their job description to be able to meet specific response times.

Motioned by Johnson/Stuchlak to approve 6 a, b,c,d,e,f,g,h, i, j and l as amended and forward with resolutions on to county board. Motion carried by unanimous voice vote.

- j. Resolution to rescind sections of administrative policy manual;

Discuss and/or act on Adams County Employee Handbook Chapter 3, Sec 1, 1.05. Kaye will send out a communication to define premise as being the building and grounds located on.

Discuss department head comments: Review of department head comments took place. Most of which have already been addressed since first submitted, some of which are currently being taken care of. Budget forms that are repetitive will be cleaned up in the near future. The hiring process has been streamlined. Additional forms will be synced up with currently revised policy.

Discuss code of conduct resolution and policy. Remove and/or disregard as this is redundant policy language that exists throughout employee manual, county board rules and administrative policy the committee unanimously consented not to implement this.

Motioned by Stuchlak/Johnson to adjourn at 3:51 p.m. Motion to adjourn carried by unanimous voice vote.

Respectfully submitted,



Cindy Philippi
Recording Secretary