

**REGULAR SESSION
DECEMBER 17, 2012**

The Trempealeau County Board of Supervisors met in Regular Session at the Government Center in the City of Whitehall, County of Trempealeau and State of Wisconsin on Monday, December 17, 2012 at 7:00 p.m. with Chair Ernest Vold presiding. The Pledge of Allegiance to the Flag of the United States of America was recited. Chair Vold and entire board of supervisors took a moment to wish Supervisor Arild Engelién a Happy 90th Birthday.

CALL

Dear Supervisor,

Please be advised that the Trempealeau County Board of Supervisors will meet at 7:00 p.m. on December 17, 2012 in the County Board Room. All County Board Members' Claims are due in the County Clerk's Office by noon on December 5, 2012 so they can be prepared for Audit Committee approval.

Sincerely,
/s/ Paul L. Syverson
County Clerk

Clerk Syverson read the call.

It was moved by John Aasen and seconded by David Suchla to accept the Call as read; it was unanimously carried by acclamation.

Roll was called. A quorum was met with 16 supervisors in attendance. Hensel Vold was absent.

Chair Vold announced the open meeting law requirements have been complied with through postings and notifications to the members and media.

ADOPTION OF THE AGENDA: It was moved by Dick Miller and seconded by Olin Fimreite to adopt the 11 item agenda. Motion carried unanimously by vote of acclamation to approve the agenda.

APPROVAL OF MINUTES: It was moved by Michael Nelson and seconded by David Larson to approve the November minutes. Motion carried unanimously by a vote of acclamation to approve.

APPEARANCES: SHERIFF DEPARTMENT MONTHLY REPORT: Sheriff Anderson reported the statistics for November. There were 46 bookings consisting of 39 males and 7 females. There were 37 White, 2 Black, 1 Asian and 6 Hispanic. The average daily in county population was 25.54 and the out of county average was .06. There were 6.47 people on electronic monitoring for a total of 32.07. There was no crash data available for November. There were also .93 people on Huber. Sheriff Anderson said they successfully sponsored another year of the "Christmas for Kids" program with the help of many volunteers. They provided for 102 families which included 263 kids.

WWC UPDATE –JAN HEROLD – Jan said there are 3,951 members in the consortium. The Blair/Whitehall office serves 564 members. After the storm in Blair in May, their offices are currently located in the City Center in Whitehall. Jan said the City has been very accommodating to them. As of May 29th, there is no waiting list for our area. She said the Chippewa/Eau Claire and St Croix chapter failed but the State is not saying why. The rate of reimbursement from the State per member is dropping in 2013 so less money is coming in. But, Jan said they started with nothing and they will continue to move forward regardless of this set back.

PRESENTATION – AMERICAN LEGION COUNTY COMMANDER PAUL BESELER-
Paul introduced Jeremy Nordie as the new Commander. Paul is stepping down after three years as commander and feels very confident with Jeremy taking his place. He also presented the Health Department a check for \$1,000 from the American Legion and the Arcadia Auxiliary. Sherry Rhoda, Director of the Health Department accepted the donation and said it will be used to purchase Pack N Plays, which will be provided to families with no cribs for safe sleeping. Also \$200 will go towards the fluoride based sealant program for children.

**RESOLUTION
2012-12-01**

ORDINANCE FOR THE REZONE OF LAND IN TOWN OF CALEDONIA

WHEREAS Donald Hultman and Lauri Munroe Hultman, property owners in the Town of Caledonia have requested the rezone of a parcel of land, and

WHEREAS the rezone is on approximately 5.0 acres, and

WHEREAS a public hearing was held pursuant to Section 59.69 (5) of Wisconsin Statutes, and

WHEREAS the Town of Caledonia supports the rezone request, and

WHEREAS the Environment and Land Use Committee moved to rezone this parcel from Residential-20 (R-20) to Transitional Agriculture (TA) and it appears that the zoning change request is appropriate under the circumstances,

THEREFORE BE IT RESOLVED that the County adopt the attached Ordinance amending the zoning district boundaries as indicated.

Dated this 17th day of December, 2012, at Whitehall, Wisconsin.

Respectfully submitted,

/s/ Tom Bice

/s/ Michael Nelson

/s/ George Brandt

/s/ Jay Low

ENVIRONMENT AND LAND USE COMMITTEE

(Ordinance is on file in the County Clerk's Office)

It was moved by Tom Bice and seconded by Michael Nelson to adopt the resolution. Roll call vote taken; motion carried with 16 yes votes; resolution adopted.

ORDINANCE
REZONE OF A PARCEL IN THE TOWN OF CALEDONIA

*The County Board of Supervisors of the County of Trempealeau does ordain as follows:
The zoning districts for Trempealeau County and zoning map shall be amended to show that the following described real estate is rezoned from Residential -20 (R20) to Transitional Agriculture (TA):*

Part of the NE ¼ of the NW ¼ of Section 31, Township 18 North, Range 8 West, further described in a Warranty Deed, Document #343736, Volume 591, Page 358 filed in the office of the Trempealeau County Register of Deeds.

Rezoned land contains approximately 5 acres.

RESOLUTION
2012-12-02

Amend Information Security and Technology Use Policy and Procedures

WHEREAS the County Board of Supervisors adopted an Information Security and Technology Use Policy and Procedures on January 15, 2001, and

WHEREAS the aforesaid policy was amended on May 18, 2009, and

WHEREAS the County desires to further amend the aforesaid policy to include a provision requiring confidentiality notices on all emails sent by County employees and to clarify required actions under the policy.

THEREFORE, BE IT RESOLVED that the attached amended Information Security and Technology Use Policy and Procedures be adopted and shall replace the existing policy.

Dated at Whitehall, Wisconsin, this 17th day of December, 2012

Respectfully submitted,
/s/ Michael Nelson
/s/ John Aasen
/s/ Tom Bice
/s/ David Suchla
/s/ Ernest Vold
EXECUTIVE/FINANCE COMMITTEE

It was moved by John Aasen and seconded by Curtis Skoyen to adopt the resolution. Roll call vote taken; motion carried with 16 yes votes; resolution adopted.

Printers, software applications, Internet access, VOIP, e-mail, personal computers, laptops, digital cameras, PDAs, plotters, scanners, mobile data terminals, squad laptops, copy machines, electronic data and databases, and the various networks.

D. Remote Access

Connection to County networks and/or systems from outside of a County building or campus location. This includes, but is not limited to, dial-up from home or other locations, client-based VPN, router-based VPN, or access to an application through the Internet.

Roles and Responsibilities

A. Trempealeau County Government

Trempealeau County Government is the organizational entity that owns, secures and establishes policy for the security of all information, resources and facilities under its control, as well as for affiliated agencies and business partners.

The County maintains the authority to take any of several steps to protect the integrity of the computer systems, and protect legitimate users from the effects of unauthorized or improper use of these facilities. These steps include the authority to limit or restrict any employee's usage of the computing facilities; the authority to inspect, copy, remove or otherwise alter any data, file, or system resources that may undermine the proper use of that system; and any other steps deemed necessary to manage and protect the County's computer facilities. This authority may be exercised with or without notice to the employee; however, whenever possible, the Information Systems Director will consult with the department head or designee prior to taking action. The County disclaims responsibility for any loss or damage to data that results from its efforts to enforce these rules or from any changes, upgrades, or maintenance of the County Technology Resources.

B. Information Systems

Information Systems Department roles and responsibilities include, but are not limited to the following:

1. Maintaining, administering, and operating all servers, infrastructure and security Equipment for Trempealeau County Government agencies.
2. Acting as the custodian of the County's Information resources and implementing the Policies regarding information security.
3. Acting on behalf of Trempealeau County Government and Department heads to Secure information, applications, systems and networks; providing authorized access to approved personnel; and monitoring, detecting, investigating and reporting on actual or suspected security breaches or incidents.
4. Acting as the gatekeeper for access to all Information Technology Resources, including Internet access. The Information Systems Department establishes the procedures for access to all information Technology Resources, including the internet and is responsible for informing the departments of these procedures.
5. Utilizing appropriate destruction methods for obsolete removable media as well as Non-removable media.

C. Department Heads

Department Heads' roles and responsibilities include, but are not limited to the following:

1. Being responsible for all electronic information in their areas, as well as stored documents and data archives. They determine who will be allowed to access their information, consistent with their policies, applicable laws, and this policy. The Department Head may delegate this authority to one other person in their organization who may act or sign on their behalf. The final responsibility for establishing clear guidance for their data and enforcing security policy lies with department heads as well as the Information Systems Department.
2. Determining application access roles and requirements and enforcing, monitoring, and managing them along with the Information Systems Department.
3. Ensuring that employees with access to Protected Health Information receive appropriate required training before authorizing access to this information.
4. Monitoring all Information Technology Resource usage by their employees to ensure it complies with all applicable laws and policies. To assist in the responsibility, Department Heads may request reports detailing Internet and Technology Resource usage from the Information Systems Department.
5. Training interns, volunteers, contractors, and other business partner's of the appropriate security and technology use for the county as outlined in this document.

D. EMPLOYEES

All employees who are provided with access to Trempealeau County electronic information are responsible for all usage of these resources. Following is a list of general responsibility statements, which are more fully detailed in other sections of this policy. Employees are responsible for:

1. Password protection,
2. Proper logout from all open applications,
3. Powering off CPU(computer) and monitor at the end of the employee's workday,
4. Store all information on the file server.
5. Understanding and complying with all Federal and State laws and regulations and County and Department policies and procedures as they apply to Information Technology use, data security, and use of protected health information (PHI) or other private information (PI),
6. Utilizing appropriate workstation physical security solutions,
7. Identifying and reporting technology use and/or security related problems and issues.
8. Users will be held accountable for all activity that occurs under their passwords and/or account name. If the Department Head, Information Systems Director and the individual person has given you permission to use their or your password or ID, you are responsible for fully documenting the times and dates of access.

Business use only

The County's Information Technology Resources shall be used for Trempealeau County Government business only.

Personal Use of Information Technology Resources

The County does not allow ANY personal use of Information Technology Resources.

Unacceptable Use of Information Technology Resources

Unacceptable use of the County's Information Technology Resources include, but are not limited to the following:

- A. Unauthorized use.
- B. Illegal purposes.
- C. Transmittal, creation, viewing, installing, downloading, and/or copying of threatening, abusive, obscene, lewd, profane or harassing material or material which suggests any lewd or lascivious act, unless such a action is required by official investigative duties.
- D. Intentionally preventing or attempting to prevent the disclosure of your identity with the intent to frighten, intimidate, threaten, abuse or harass another person.
- E. Unauthorized or improper transmittal of material that is confidential to the County, or is otherwise protected by law.
- F. Disruption of network services, such as knowingly distributing computer viruses, or actual or attempted intrusion, destruction or defacement of information (hacking or cracking).
- G. Interception or alteration of network packets.
- H. Use of someone else's identity and password for access to Information Technology resources without proper authorization.
- I. Attempt to evade, disable, or decipher passwords or other security provisions of systems on the network without proper authorization.
- J. Reproduction and/or distribution of copyrighted materials without proper authorization.
- K. Allowing non-authorized individuals to access or use Information Technology Resources
- L. Attaching personal networking devices to the County network.
- M. Disabling or interfering with the County-installed anti-virus systems.

Ethics Conflicts

Information Technology Resources shall not be used for commercial ventures, personal gain, religious or political causes.

Authorization of Use

Employees are to be provided access to County Information Technology Resources only if authorized by the appropriate department head or designee. Employees should be granted the minimum level of access to networks, information, and technology required to perform their job responsibilities. All access that is not specifically permitted is denied.

County Access

The County reserves, and intends to exercise its right, as is reasonably necessary, to search, review, audit, monitor, intercept or access an employee's use of the Information Technology resources provided to him/her.

Work Product

All work products created through the use of Information Technology Resources are the property of Trempealeau County Government. Any materials developed, composed, sent or received, using County provided Information Technology Resources are, and will, remain the property of the County.

Privacy

Employees do not have an expectation of privacy regarding the use of Information Technology Resources regardless of the assignment or creation of passwords, ID numbers or access codes.

Harassing or Discriminatory Behavior

The Trempealeau County Information Technology Resources shall not be used for discriminatory harassing, obscene, or other inappropriate communications.

Reproduction and/or Dissemination of Materials

Reproduction and/or dissemination of materials in any form, or on any media, must be consistent with copyright laws. Proper authorization must be obtained prior to the reproduction and/or dissemination of materials that are not subject to copyright laws but are otherwise confidential or restricted.

Federal, State, local laws and regulation

Usage of Trempealeau County Information Technology Resources shall not violate applicable Federal, state, and local laws and regulations.

Electronic Documents as Public Record

All electronic documents, including E-mail, may be considered a public record, and as such may be open to public inspection upon request.

Administration and Enforcement of this Policy

Administration and enforcement of the provisions contained herein shall be the responsibility of the employee's immediate supervisor and/or Information Systems Director and in turn, the department head.

E-mail Use

The following items apply specifically to the use of E-mail on Trempealeau County Government systems:

- A. E-mail is not a secured media, except inside the County's E-mail system. Any E-mail that can be sent out of the County's E-mail system, should be considered non-secure. A special encrypted E-Mail system exists which is used to pass protected information outside of the County.
- B. E-mail is subject to applicable privacy, security, and records retention laws and guidelines for the information that a particular message contains. As such, E-Mail records must be appropriately secured and retained.

- C. No employee shall e-mail sensitive, personal or private information, unless it is authorized and sent by approved methods.
- D. Employees shall not open unusual looking or unexpected E-Mail. E-Mail is often used by others for illegal purposes and may contain computer viruses.
- E. Employees shall not respond to E-Mail requesting personal or banking information, or requesting user ID's or passwords.
- F. If an employee has any doubt about the authenticity of an E-Mail, or about what the E-Mail is requesting, the employee must notify their supervisor and/or Information Systems Department immediately.
- G. Except as provided in paragraph H. below, all employees shall have the following confidentiality notice in every email that is sent:
 - a. CONFIDENTIALITY NOTICE: This e-mail, including any attachments, may contain confidential, privileged and/or proprietary information. Disclosure of this email, including any attachments, is strictly limited to the recipient intended by the sender of this message. Receipt by anyone other than the intended recipient does not constitute waiver or loss of the confidential or privileged nature of the communication. Any review, use, disclosure, or retention by others is strictly prohibited. If you are not an intended recipient or you have received this e-mail message in error, please contact the sender and delete this e-mail, any attachments, and all copies.
- H. Any employee providing legal advice (attorney) shall have the following Confidentiality Notice in every email that is sent:
 - a. CONFIDENTIALITY NOTICE: This e-mail message may contain information which is subject to the attorney-client privilege and/or attorney work-product doctrine and therefore confidential. Disclosure of this email, including any attachments, is strictly limited to the recipient intended by the sender of this message. Receipt by anyone other than the intended recipient does not constitute waiver or loss of the confidential or privileged nature of the communication. Any unauthorized review, disclosure, dissemination, duplication or use is prohibited. If you are not the intended recipient or you have received this e-mail message in error, please notify this office immediately and delete or destroy the original and all copies.

Internet use

Internet resources are provided to employees in an effort to allow them to be more efficient, productive, and to have access to information that is necessary for them to carry out their responsibilities as an employee of the County. Employees are expected and required to use the Internet in a manner consistent with their position and work responsibilities with the County. Approval of the employee's department head (designee) is required to get access to the Internet. Inappropriate use of the County's internet resources may result in discipline up to and including discharge of employment. In addition, the employee may be subject to civil and/or criminal penalties.

The following items apply specifically to the use of the Internet:

- A. All Internet users are responsible to ensure they are in compliance with all applicable laws and County policies, including computer security, virus detection, and access to questionable sites and/or material.
- B. Under no circumstances shall the Internet be used to access lewd, objectionable, pornographic sexually explicit, or illegal materials, or sites that are sponsored by or contain materials regarding discrimination, hate groups, or gambling. The only exception is when such access is used to perform official investigations, required in the course of one's work, and approved by the Department head.
- C. Internet access requires authentication through the firewall to ensure that only authorized employees may access the Internet.
- D. Streaming media should only be used for official or training purposes. The Internet shall not be used to listen to radio or tv broadcasts for entertainment.
- E. Instant messaging is not allowed, except for that which is provided by the County's E-Mail system.
- F. Employees shall not purchase any items on the Internet from any County workstation or network connection using a personal credit or debit card, unless that transaction is for County business(such as purchasing plane tickets or to guarantee a hotel room for a conference).
- G. Employees shall exercise caution when prompted to enter information which will identify them or the networking architecture of the County. If there is any question regarding the legitimacy of the site or the information being requested, the employee must notify their supervisor or contact the Information Systems Department before proceeding. Employees accept all risk when entering personal, medical, or financial information of any kind on external websites.
- H. Employees shall not download programs or plug-ins from the Internet unless authorized to do so by the Information Systems Department. Such actions could download viruses or other malicious code, or could violate licensing and copyright laws.
- I. File downloads such as *.pdf files, word documents, research materials, etc are permissible. All downloaded files shall be checked for viruses.
- J. The Internet shall not be used to attack or test the security of other systems.

Password Use

Computer passwords shall be of sufficient strength so as not to be easily cracked or broken by unauthorized individuals, and to ensure the safety of the information and networks within Trempealeau County Government. The Information Systems department will establish and communicate specific requirements for password content.

The following items apply specifically to password use:

- A. Each user shall have his/her own, unique login account and password. No default user ID or password will be permitted on any system.
- B. Passwords shall not be written down and stored on or near computer equipment.
- C. Passwords shall not be stored in clear view.
- D. Under no circumstances shall employees share, or be required to share, login credentials, normally defined as the combination of both their user ID and password.
- E. Employees do not have expectation of privacy regarding the use of E-Mail on County systems regardless of the assignment of passwords, ID numbers or access codes.
- F. Passwords must be changed every six months.

Workstation Physical Security

Employees are responsible for maintaining the physical security of their desktop workstations, portable computing devices, and removable media (such as diskettes and CD's) by restricting and controlling physical access to these items. This can be accomplished by utilizing one or more of the following physical security solutions:

- A. Properly positioning and protecting systems such that the information cannot easily be read or obtained.
- B. Monitors should generally be kept from the plain view of anyone who does not have the appropriate security access or clearance to information that may be displayed. Make sure that monitors cannot be viewed through outside windows, from public hallways, from public reception areas, or by reflection off other objects.
- C. Turn monitors away from counter areas.
- D. Utilize a special shade or polarizing monitor filter, when necessary.
- E. Keep keyboard, mouse, and other components far enough away from public so they cannot be tampered with or stolen.
- F. Printers should be kept in protected areas to keep sensitive information from being disclosed inappropriately.
- G. Printed materials from any source should be kept secure, away from viewing, and out of public reach.
- H. Many workstations may utilize a locked down configuration where the user will not have local administrator rights on his or her own workstation to prevent the installation of unauthorized software.
- I. Workstations may utilize an automatic screensaver that is password protected and which activates after a set period of inactivity. Where this solution has been implemented or required, departments or employees shall take no action to disable or prolong the set time frame of this screensaver.
- J. Removable media will have the same security requirements as the highest sensitivity of information on that device, and should be stored and secured as such.
- K. Since most County information is network accessible, there should be minimal need to copy data to removable media.
- L. All media storage devices shall be destroyed when it has been determined that they are no longer of use and must not be discarded in the trash.

Security and Confidentiality of Electronic Private Information

All employees are required to comply with state and federal laws and regulations, as well as County and Department procedures and policies regarding the use and security of electronic

protected health information(ePHI), and proprietary, sensitive, personal, or confidential information, all of which is herein after referred to as Private Information(PI). Failure to comply will result in discipline up to and including termination of employment. In addition, the employee may be subject to civil and/or criminal penalties.

HIPAA Security Polices and Procedures

Employees who have access to electronic protected health information(ePHI) have the responsibility to follow all documented HIPAA security and privacy practices, procedures and policies provided by Trempealeau County. Employees must keep desktop computers, and all portable computers, physically secure and prevent them from being accessed by unauthorized users. Employees must keep ePHI data from being read by or distributed to unauthorized users.

Failure to comply with HIPAA requirements will also result in an employee being subject to the provisions of the HIPAA Sanctions Policy. In addition, the employee may be subject to civil and/or criminal penalties.

Security of Private Information (PI)

Trempealeau County Government is responsible for providing employees with the means to keep PI secure. Trempealeau County Government is also responsible for providing secure access to PI data.

Employees shall keep PI safe, private, and unavailable to employees and non-employees who have no business need to access PI. This may be accomplished by:

- A. Utilizing all appropriate workstation physical security measures as outlined in the workstation physical security section of this policy such as invoking the automatic screensaver, using monitor filters or enclosures, or positioning the monitor so it cannot be viewed by unauthorized individuals:
- B. Logging out or locking the workstation before leaving the computer unattended.
- C. By applying all Trempealeau County PI security and privacy policies and practices learned through training.
- D. By logging off and powering down all computer workstations at the end of workday.

Secure Computers When Not in Use

Employees shall secure computers when not in use, by using technical solutions supplied by Trempealeau County Information Systems department, that ensure only authorized users operate computers that have access to PI. Employees shall be provided with unique user IDs and shall be required to use network and application passwords to gain access to PI.

Destruction of Obsolete Removable Media Containing PI

Subject to applicable record retention laws and schedules, employees shall contact the Information Systems department for destruction of removable media and all obsolete removable media containing PI or other information requiring protection.

Computer Hardware/Software Usage

The following items specifically apply to the use of Trempealeau County Government computer

hardware and software.

A. **Personal Use of County Computer Hardware and Software**

Employees shall not be granted permission to use County computer hardware/software for personal purposes. Copying and use of County-owned software is not permitted without proper authorization from the Information Systems Department and Department head, in compliance with all applicable laws, policies and procedures.

B. **Alterations of Computer Hardware**

County-owned computer equipment must not be altered in any way, i.e. removing or adding CD-ROM drives, video cards, memory, etc.

C. **Disposal of Obsolete Hardware and Software**

Information Systems Department is solely responsible for the proper disposal of all County-owned software and hardware. Departments shall contact the Information Systems Department for proper disposal.

1. Servers will generally not be re-commissioned for other use until an evaluation is completed to determine that residual data requiring special security considerations have been deleted. Certificate of Disposal form filled out and signed by the IS Department is required.
2. No media shall be disposed of without being erased, degaussed and/or destroyed first. The IS Department shall prepare all decommissioned computer equipment for disposal. Certificate of Disposal form filled out and signed by the IS Department is required.
 - a. All hard drives must be cleaned with software that is DoD 5220.22-M and Gutmann method compliant(The Gutmann method is an algorithm for securely erasing the contents of computer hard drives, such as files).
 - b. All saleable PC equipment shall have the hard drives taken out and destroyed before they are sold or donated. Certificate of Disposal form filled out and signed by the IS Department is required. The person purchasing or receiving said equipment, must sign the Trempealeau County Property Purchase Disclaimer before receiving their equipment.
 - c. Non-saleable equipment shall be disposed of in accordance with applicable statutes, and ordinances governing disposal and recycling of computer and computer related equipment. Certificate of Disposal form filled out and signed by the IS Department is required.

D. **Software Installed on County Computers**

Only software purchased by the Information Systems Department and properly licensed to

the County shall be installed on County computers. All installations shall be done by Information Systems staff or authorized department staff. The use of this software must be in compliance with the manufacturers license agreement and cannot be copied to multiple computers unless permitted by the license agreement. Unauthorized software(such as shareware, freeware, or employee-owned software) can only be installed on County computers by and with the approval of the Information Systems Department staff.

E. **Compliance with Software Copyright Laws**

Use of computer software is subject to Federal copyright laws. Copying and using software

without explicit permission from the copyright owner constitutes copyright infringement. Employees who willfully and knowingly infringe a software copyright by making, acquiring, installing, downloading, or using unauthorized copies of computer software shall be subject to discipline up to and including termination of employment. In addition, criminal and/or civil penalties may apply.

F. Unauthorized Software

Trempealeau County prohibits the following types of computer software from being installed and/or used on County computers unless approved and installed by the Information Systems department:

1. Games – including Microsoft games that are included with the Microsoft operating System.
2. Demonstration or evaluation software
3. Interactive internet games
4. Employee-owned software
5. Freeware
6. Shareware
7. Instant messaging software – all exterior Instant Messaging Services are prohibited.
8. Chat room / Chat channels –acceptable only if used for verifiable business purposes.
9. Streaming Software.

G. Software Audit

To ensure that Trempealeau County Government is in compliance with the US Copyright law, Information Systems Department shall conduct a periodic electronic software audit of all workstations and Servers owned by the County. These audits shall be conducted with or without notice to employees. If unauthorized software is found, it shall be removed from computers and Department Heads or designees will be informed of the removal.

H. Removal of Unauthorized Software

Information Systems Department shall remove all unauthorized software that has been installed on any County computer or other Information Technology device following the steps outlined below:

1. The specific PC or device with the unauthorized software will be identified through the electronic software or by other means.
2. Information Systems will contact the user and/or Department Head(designee) to determine if there is a legitimate business reason why the unauthorized software has been installed on a County computer.
3. If the Department Head(designee) indicates that the unauthorized software is needed for the employee to do their job, the following process must be used.
 - a. The Department head must request the software be purchased and installed by the Information Systems Department.
 - b. If the software was installed by the department/employee, the unauthorized

software will be automatically removed and a message will be sent to the Department Head(designee).

I. Copying Software Disks and Manuals

The copying of software disks and manuals is strictly prohibited unless it is authorized by the Information Systems Department as well as by the associated software license agreement, or received through written correspondence with the software owners.

J. Use of State-Provided Computers and Software

Employees who are assigned to use a State-provided PC or who utilize software provided by the State are required to comply with all State policies and procedures.

Incident Reporting

Employees have a responsibility to report any actual or suspected information or network security incidents to their direct supervisor or Department Head(designee) and in turn shall report the incident to the Information Systems Director.

A. Types of Incidents Which Must Be Reported

The following types of incidents are examples of situations that must be reported as a possible security incident:

1. Unauthorized release of information in an E-Mail, whether intentional or accidental
2. Unauthorized receipt of any E-Mail containing information that is protected from disclosure(such as health care information).
3. Receipt of E-Mail that looks to be illegal or contains sexually explicit, hate-group related, or otherwise illegal material.
4. Suspicion that your password has been disclosed or that someone may have been using one of your login credentials or accounts.
5. Receipt of any E-Mail that triggers your anti-virus software.
6. Any individual who asks you for your password, or to use your account to review the contents of your E-Mail.
7. Computer attacks coming from outside the County, or any suspected virus, worm, or other malicious code.
8. Theft or unauthorized removal of media, data, storage devices, disks, or CDs
9. Unauthorized access to the County's computer system(s) by a third party.
10. Inappropriate use of the County's Information Technology Resources. Examples include, but are not limited to , access of inappropriate web sites; using County systems for inappropriate, non-work related materials; abusing County systems or using them for unintended purposes; using workstations, servers, or other devices to attempt to monitor, detect passwords, probe systems or networks, or other such hacking/cracking activities.

B. Incident Reporting Procedures

Employees shall use one of the following options to report an actual or suspected security incident:

1. Report the incident to your supervisor or manager.
2. Send an e-mail to the County Information Systems Director, describing the incident.
3. Call the County Information Systems Director to report an incident

Incidents shall be investigated by the County's Information Systems Director. In addition, if the security incident involves ePHI, the Human Resources Department shall be notified so that an investigation can be conducted under the provisions of the HIPPA policy.

Procedure when employee changes or leaves a position

The following procedures will be followed when an employee retires, resigns, transfers, bumping, termination, etc in regards to Information Technology Resources:

- A. **Requirements for New and/or Departing Employees** – Forms are required for:
1. **New and/or transferred Employees Network Access** – Each department is required to notify the IS Department at least 1 week in advance of new/transferring employees hire/transfer date. Information Systems Employee Access Authorization form must be completed, signed by Department Head, and submitted to IS by this time, when possible. The Information Systems Access Authorization form defines the employees permission to access the Countys Information Technology resources. All new and or transferred employees must sign the Security and Technology Use Policy and procedures acknowledgement form.
3. **Departing /bumped Employees** - Each department is required to give the IS Department at least one week notice of employees departing employment. An Information Systems employee Access Authorization form must be completed and signed by the department head by this time. The Information Systems Employee Authorization form defines to the IS department when the user profiles shall be disabled and/or deleted and how the user's data files and old email should be handled, as well as how they want to handle all the other Technology resources that the employee had access to.
4. **Securing equipment** - When a employee leaves a position for any reason, the Information Systems Director and/or Personnel Director may deem it necessary to remove their Technology Resources that were assigned to them(like a computer) and put said equipment in a secure locked room within the IS Department until such time that the equipment is cleared of any issues there may be.
- B. **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 shall be changed prior to a new person using the profile. When the profile is not used, the Information Systems Department will disable it.

Violation of the terms and conditions contained in this policy may result in disciplinary actions, up to and including discharge, and termination or limitations of access for the violator to any one or all Information Technology Resources.

**SECURITY AND TECHNOLOGY USE POLICY AND PROCEDURES
ACKNOWLEDGEMENT**

As an employee of Trempealeau County, I acknowledge that I have read and understand the County's Computer, Internal Network, Electronic Mail and Internet policies and procedures guidelines contained in the Information Security and Technology Use Policy and Procedures document.

I am aware that violation of the guidelines may be the basis for disciplinary actions, up to and including discharge from employment.

I am aware that the County retains exclusive ownership of respective documents, applications, and messages created using information technology resources that are provided.

I am aware that the County reserves and will exercise the right to review, audit, intercept, access and disclose all matters on the County's Internal/External Network at any time when legitimate business needs require it. I am aware that the County may exercise these rights with or without employee notice, and that such access may occur during or after working hours.

I am aware that use of a County-provided password or code does not guarantee confidentiality, privacy, or restrict the County's right to access electronic communications.

I acknowledge that I have read and understand this notice.

Employee: _____

Date: _____

INFORMATION SYSTEMS EMPLOYEE ACCESS AUTHORIZATION FORM

Supervisors and/or Department head: Please fill out and sign the following form (at least one week prior to the employee's first day for new or transferring, one week prior to an employee leaving a position for ANY REASON)

Employee new and/or transferred- Departing- bumped - retirement - resignation - termination etc			
Employee Name:		Department:	
Date Hired:		Department head or (designee) name (please print)	
Department head or designee signature:	Date:		Office phone:
Note(Do you want old profiles deleted?)			
New employee user ID and password or employee transferring or bumped new ID and password(if the same as their current one still fill out the user name and password). If not the same please list new ID and Password.	User ID:		
	Password:		
If New employee please list what they want for external email address and if they should have	External email address	@tremplounty.com	

permission to have Internal email. If leaving a position and going to a new position within the county will they use their current internal and external email? If not please list the new external email and if they will have permission to use internal email.	Internal email	Permission to have(circle one) yes no
Employee needs access to or will need to return any of the following. Please check all that apply:		
Computer	Where will this be located? Department?	
Laptop	Where will this be located?	
Printer	Circle one	Color, B&W, or department shared printer
PDA	Type and what application to synchronize?	
Internet access (yes or no)	Restrict sites? please list	
If transferring is the equipment going with the employee?		
Add/Cancel specific software access (accounting software, HR software, GCS, Rims, etc.)		
Add/Remove name from department email groups/directories(which department). If transferring which department group will their email be under.		
If transferring, any additional requests for what to do with old equipment/software/etc? Date that you want this done by?		
When a employee leaves a position for any reason, the Information Systems Director and/or Personnel Director may deem it necessary to remove their Technology Resources that were assigned to them(like a computer) and put said equipment in a secure locked room within the IS Department until such time that the equipment is cleared of any issues there may be/etc? Date that you want this done by? Give explanation of what will done and why.		

Certificate of Disposal
Information Technology Resources
Information Systems Department

Date:	
-------	--

Department:		Employee:	
-------------	--	-----------	--

Equipment model/name:		Equipment Serial number:	
-----------------------	--	--------------------------	--

Hard drive model/name:		Hard Drive serial number:
------------------------	--	---------------------------

Software name/version:		Other equipment name/version:
------------------------	--	-------------------------------

Method of disposal:	
---------------------	--

Further notes and comments:	
-----------------------------	--

IS employee Disposing of equipment:		IS Employee signature:
-------------------------------------	--	------------------------

IS Director name:		IS Director signature:
-------------------	--	------------------------

Information Systems certifies that the above equipment has been properly disposed of and/or destroyed in accordance to all applicable Federal, State and Local Rules and Regulations.

Information Systems acknowledges, all electronic data on functional storage devices have been or will be overwritten by means of a destructive write process using a program that performs an overwrite of data on the hard drive. IS further acknowledges that all storage devices deemed to be non-functional have been or will be shredded or otherwise destroyed after removal of all data. All storage devices will be removed and destroyed before the equipment it was stored in is sold/donated. Non-saleable equipment will be disposed of in accordance with applicable statutes, and ordinances governing disposal and recycling of computer and computer related equipment.

**RESOLUTION
2012-12-03**

TREMPEALEAU COUNTY HEALTH DEPARTMENT

Additional Public Health Funds

WHEREAS the Health Department original budget did not provide for increases in anticipated revenues in funding for existing programs, and

WHEREAS these additional funds generate additional expenditures not budgeted for, and

WHEREAS these additional funds will not require additional county appropriations, and

Account Number	Account Name	Amount	Amount
201. 43558	GRANT – Adult Health Prevention	\$ 3,543.00	
201.54162.111	Wages		\$ 2398.66
201.54162.151	Social Security		\$ 148.72
201.54162.152	Retirement		\$ 160.71
201.54162.153	Medicare		\$ 34.78
201.54162.154	Health Insurance		\$ 609.50
201.54162.225	Telephone		\$ 100.00
201.54162.310	Office Supplies		\$ 40.63
201.54162.339	Mileage		\$ 50.00

NOW THEREFORE, BE IT RESOLVED, that the aforementioned revenues to be added to the anticipated revenue account and budget expenditure account as shown.

BE IT FURTHER RESOLVED that the Trempealeau County Board of Supervisors hereby creates a Non-lapsing account as follows in the Trempealeau County Health Department, in order to develop a Performance Management System and/or Quality Improvement Plan to enhance local public health movement toward accreditation.

Dated at Whitehall, Wisconsin this 17th day of December 2012

Respectfully submitted,
 /s/ George Brandt
 /s/ Dr. J Selkurt
 /s/ Sally Miller
 /s/ John Aasen
 /s/ Jay Low
 /s/ Dr. William Baxa
 /s/ David Larson
 /s/ Pamela Nelson
 BOARD OF HEALTH COMMITTEE

It was moved by George Brandt and seconded by Douglas Winters to adopt the resolution. Roll call taken; motion carried with 16 yes votes; resolution adopted.

**RESOLUTION
 2012-12-04**

Increase Department of Human Services Assigned Non-lapsing Contingency Fund Ceiling

WHEREAS the Trempealeau County Board of Supervisors prior to 2009 authorized a Unified Board Contingency Fund ceiling of \$300,000.00, and

WHEREAS the Trempealeau County Board of Supervisors prior to 2009 authorized a Department of Social Services Contingency Fund ceiling of \$200,000.00, and

WHEREAS on November 1, 2008, Unified Board and Social Services were merged and a new agency titled the Trempealeau County Department of Human Services was established pursuant to Chapter 46.23 (3), and

WHEREAS the Trempealeau County Board of Supervisors at the September, 2009 County Board Meeting passed a resolution establishing a \$300,000.00 contingency fund ceiling for the Department of Human Services, and

WHEREAS as a result of unexpected expenses and subsequent budget overruns in FY2010, the Department of Human Services contingency fund balance was reduced to \$24,234.00, and

WHEREAS as a result of program changes and fiscal management of services in FY2011, the Department of Human Services contingency fund was restored to \$288,806.00 at the end of year, and

WHEREAS it is prudent and fiscally responsible to continue a Department of Human Services contingency fund and to increase the maximum amount in that fund for unexpected expenses in future years so as not to burden the general fund.

NOW THEREFORE BE IT RESOLVED that the Trempealeau County Board of Supervisors increase the maximum amount of funds that may be held in the Department of Human Services assigned non-lapsing contingency fund to \$500,000.00

BE IT FURTHER RESOLVED that only those surplus monies left over in the Human Services budget at the end of the year be placed in the Department of Human Services assigned contingency fund.

Dated at Whitehall, Wisconsin this 17th day of December, 2012.

Respectfully submitted,

/s/ Michelle Haines

/s/ Robert Reichwein

/s/ Arild Engelién

/s/ Curtis Skoyen

HUMAN SERVICES BOARD

/s/ Michael Nelson

/s/ Ernest Vold

/s/ John Aasen

/s/ David Suchla

/s/ Tom Bice

EXECUTIVE/FINANCE COMMITTEE

It was moved by David Suchla and seconded by Michael Nelson to adopt the resolution. Roll call vote taken; motion carried with 16 yes votes; resolution adopted.

**RESOLUTION
2012-12-05**

Approval of a Half-time Social Worker position in Human Services

WHEREAS the Human Services Department provides services and counseling through the Aging & Disability Resource Center (ADRC) for information, assistance and long term care options for our maturing population, and

WHEREAS the ADRC has received increasing numbers of referrals and requests for assistance by residents in Trempealeau County who wish to transition from nursing homes, and

WHEREAS these services provide assistance looking for alternative housing options, allowing for people who currently live in nursing home facilities to transition to independence living options, and

WHEREAS Trempealeau County has eight nursing homes currently operating in the County, and

WHEREAS this has increased demands to meet with new and existing residents to assist those who wish to return to the community, and

WHEREAS a Half-time Social Worker is needed to assist residents research all options, and

WHEREAS this position will be funded by reimbursement from State and Federal funds with no attached county levy, and

WHEREAS this new position has been reviewed and approved by the Human Services Board, Personnel/Bargaining Committee and the Executive/Finance Committee.

NOW THEREFORE BE IT RESOLVED that the Trempealeau County Board approve the creation of a half-time Social Worker position in the Department of Human Services, and

BE IT FURTHER RESOLVED that this position be subject to the terms of the Social Services Professional Union contract.

Dated at Whitehall, Wisconsin this 17th day of December, 2012.

Respectfully submitted,

/s/ Michelle Haines
/s/ Arild Engelién
/s/ Robert Reichwein
/s/ Curtis Skoyen
HUMAN SERVICES
COMMITTEE

/s/ Dick Miller
/s/ Douglas Winters
/s/ Tom Bice
/s/ Robert Reichwein
/s/ Ernest Vold
PERSONNEL/BARGAINING
COMMITTEE

/s/ Michael Nelson
/s/ Tom Bice
/s/ John Aasen
/s/ David Suchla
/s/ Ernest Vold
EXECUTIVE/FINANCE
COMMITTEE

It was moved by Arild Engelién and seconded by Curtis Skoyen to adopt the resolution. Roll call vote taken; motion carried with 16 yes votes; resolution adopted.

**RESOLUTION
2012-12-06**

WIC Director/Public Health Nutritionist Position- Change Hours/Pay Grade

WHEREAS the pay for the WIC Director/Public Health Nutritionist position was increased from a wage grade 7C in August, 2008, and again increased to a grade 9 of the Courthouse Union wage schedule in November, 2008, due to inability to recruit candidates, and

WHEREAS funding for the WIC program could only support staffing the position at grade 9 for only 32 hours per week, and

WHEREAS there has been continuous increases in demand for services this program offers, and

WHEREAS the demands for services of the program require the position to increase to 40 hours per week, and

WHEREAS funding for this program is anticipated to decrease and will not be able to support the increase to 40 hours at the current pay grade 9, and

WHEREAS restoring the positions original pay grade would allow for the program to fund the position at a 7C, and increasing the number of hours per week up to 40 hours, and

WHEREAS due to a resignation of the WIC Director/Public Health Nutritionist, the department has opportunity to make the changes to the position in order to strengthen the program's community outreach.

NOW THEREFORE BE IT RESOLVED that the WIC Director/Public Health Nutritionist position be reverted back to a grade 7C (\$19.9131/hr) and staffed up to 40 hours per week, effective 1/1/2013.

Dated at Whitehall, Wisconsin this 17th day of December, 2012.

Respectfully submitted,

/s/ George Brandt

/s/ John Aasen

/s/ Sally Miller

/s/ Jay Low

/s/ David Larson

BOARD OF HEALTH

COMMITTEE

/s/ Michael Nelson

/s/ Ernest Vold

/s/ John Aasen

/s/ David Suchla

/s/ Tom Bice

EXECUTIVE/FINANCE

COMMITTEE

/s/ Dick Miller

/s/ Douglas Winters

/s/ Tom Bice

/s/ Robert Reichwein

/s/ Ernest Vold

PERSONNEL/BARGAINING

COMMITTEE

It was moved by George Brandt and seconded by Olin Fimreite to adopt the resolution. Roll call vote taken; motion carried with 16 yes votes; resolution adopted.

RESOLUTION

2012-12-07

REPORT – CLAIMS OF MEMBERS

Your Audit Committee hereby respectfully reports that they have audited the following claims and recommend that they be allowed as follows:

NAME	PER DIEM	EXPENSES	TOTAL
John Aasen	\$140.00	\$24.42	\$164.42
Tom Bice	\$140.00	\$119.88	\$259.88

George Brandt	\$105.00	\$81.03	\$186.03
Arild Engelién	\$140.00	\$142.08	\$282.08
Olin Fimreite	\$105.00	\$0.00	\$105.00
Michelle Haines	\$70.00	\$27.76	\$97.76
David Larson	\$70.00	\$48.84	\$118.84
Jay Low	\$105.00	\$69.38	\$174.38
Dick Miller	\$140.00	\$53.28	\$193.28
Sally Miller	\$105.00	\$57.72	\$162.72
Michael Nelson	\$175.00	\$63.27	\$238.27
Robert Reichwein	\$105.00	\$53.28	\$158.28
Curtis Skoyen	\$175.00	\$98.81	\$273.81
David Suchla	\$105.00	\$23.31	\$128.31
Ernest Vold	\$280.00	\$158.73	\$438.73
Hensel Vold	\$0.00	\$0.00	\$0.00
Douglas Winters	<u>\$175.00</u>	<u>\$130.98</u>	<u>\$305.98</u>
TOTALS	\$2,135.00	\$1,152.77	\$3,287.77
YTD Totals	\$31,140.00	\$14,610.79	\$45,750.79

Dated at Whitehall, Wisconsin, this 17th day of December, 2012

Respectfully submitted,
/s/ Ernest Vold
/s/ Michael Nelson
/s/ Douglas Winters
AUDIT COMMITTEE

It was moved by John Aasen and seconded by David Larson to adopt the resolution. Roll call vote taken; motion carried with 16 yes votes; resolution adopted.

ANNOUNCEMENT/APPOINTMENTS/ELECTIONS: APPOINTMENT TO TRANSPORTATION COORDINATION COMMITTEE: Chair Vold requested the reappointment of Mary Gullicksrud to the Transportation Coordination Committee and also to re-appoint Duane

Sackett to the Aging Advisory Council. John Aasen made a motion to approve the re-appointments and Olin Fimreite seconded it. Motion carried unanimously to approve the reappointments.

APPOINTMENT TO VETERAN’S SERVICE COMMISSION: Chair Vold requested the re-appointment of Robert Hageness to the Veteran’s Service Commission for another 3 year term. Michael Nelson made a motion to approve the re-appointment and Curtis Skoyen seconded it. Motion carried unanimously to approve the re-appointment.

APPOINTMENT TO HOUSING AUTHORITY OF TREMPEALEAU COUNTY: Chair Vold requested the re-appointment of Duane Fredrick to the Housing Authority Board for another 5 year term. Olin Fimreite made a motion to approve the re-appointment and George Brandt seconded it. Motion carried unanimously to approve the re-appointment.

Chair Vold would like approval to create and appoint a Strategic Planning Committee for Programs and Facilities for Law Enforcement in the County. He included a list of names and positions that he would like to see serve on the committee. Olin Fimreite made a motion to approve the appointments on the list and Dick Miller seconded it. George Brandt had some questions. This committee will look at efficiencies in the Sheriff Department and the board members appointed will receive per diem and mileage from the County Board budget. They don’t anticipate too many meetings to accomplish their goals.

COMMITTEE REPORTS: EXECUTIVE & FINANCE COMMITTEE BUDGET UPDATE REPORT: Chair Vold said everyone has a copy of the budget on their desk and if there are any questions, contact the clerk.

CORRESPONDENCE: There was none for December.

CLOSING: It was moved by Douglas Winters and seconded by Dick Miller to instruct the Clerk to pay mileage and per diem; roll call vote; motion carried with 16 yes votes.

ADJOURNMENT: Michael Nelson made a motion to adjourn the meeting and Curtis Skoyen seconded it. Motion carried unanimously. Chair Vold declared the meeting adjourned until January 21, 2013 at 7 p.m. The meeting was adjourned at 7:58 pm.

Recording Secretary,
Mary Martin

Dist #	SUPERVISOR	PER DIEM	# Of MILES	MILEAGE
1	ARILD ENGELIEN	\$70.00	64	\$35.52
2	DOUGLAS WINTERS	\$70.00	60	\$33.30
3	SALLY MILLER	\$70.00	52	\$28.86
4	JAY LOW	\$70.00	50	\$27.75
5	TOM BICE	\$70.00	54	\$29.97
6	GEORGE BRANDT	\$70.00	34	\$18.87

7	ROBERT REICHWEIN	\$70.00	32	\$17.76
8	DICK MILLER	\$70.00	24	\$13.32
9	MICHELLE HAINES	\$70.00	25	\$13.88
10	JOHN AASEN	\$70.00	10	\$5.55
11	DAVID SUCHLA	\$70.00	14	\$7.77
12	DAVID LARSON	\$70.00	46	\$25.53
13	OLIN FIMREITE	\$70.00	2	\$1.11
14	MICHAEL NELSON	\$70.00	22	\$12.21
15	HENSEL VOLD	\$0.00	0	\$0.00
16	CURTIS SKOYEN	\$70.00	33	\$18.32
17	ERNEST VOLD	<u>\$70.00</u>	<u>38</u>	<u>\$21.09</u>
	TOTALS	\$1,120.00	560	\$ 310.81