

Polk County Wisconsin

COMPUTER POLICIES AND PROCEDURE

Policy 901

Effective Date: 04-29-93

Revision Date: 6-21-05

I. Purpose

- a) The purpose of these policies and procedures is to ensure the safety of the investment Polk County has made in computer hardware, software, training, and labor.

II. Background

- a) Data processing information has become a vital resource of the County and is critical to the day-to-day operation of the County. This information, like any other asset, must be protected.
- b) As Personal Computers and Local Area Networks are used increasingly in County employees daily activities, it becomes increasingly important that these tools be used properly and efficiently.

III. Responsibilities

- a) It is the responsibility of each department head to implement each of these policies, educate their employees, and monitor their compliance.
- b) The Information Technology Department, which is governed by the Finance Committee, will develop and maintain the Computer Policies and Procedures. It will be their responsibility to audit end users periodically to ensure that the policies have been implemented properly and procedures are being followed correctly.

IV. Ownership of Computer Hardware, Software, and Information

- a) All computer hardware purchased by the County is the property of the County and under the ultimate control of the Information Technology Department, who will coordinate the reallocation of excess hardware.
 1. The Information Technology Department can reallocate any County hardware that has been identified as excess by Department Heads.
 2. The Information Technology Department will manage and track the inventory, allocation, licensure, registration, and documentation of all hardware.
 3. Each Department is responsible for listing the hardware allocated to their department on the County insurance inventory for their department.

- b) All computer software purchased or developed by the County is the property of the County and under the ultimate control, as listed below;
1. Proprietary software, which is specific software used by specific department(s), for a specific function, shall be under the control of that department or departments.
 - a. Each department who controls proprietary software, shall be responsible to designate a person or persons to manage and track current and accurate inventory, allocation, registration, licensure, and documentation of such proprietary software
 2. Global software, which is software used by all or most departments shall be under the control of the Information Technology Department
 - a. The Information Technology Department will designate a Technical Support Specialist to manage and track current and accurate inventory, allocation, registration, licensure, and documentation of such global software
 3. Each Department is responsible for listing the software allocated to their department on the County insurance inventory for their department. Undistributed software licenses will be kept on the I.T. Department's insurance inventory.

V. Use of County Purchased Hardware and Software

- a) Employees will not remove any hardware or software from their work locations without the expressed prior consent of their supervisors. Failure to comply with this policy could be construed as employee theft and become grounds for dismissal or other disciplinary action.
- b) Employees will not install County-owned hardware and software onto, or into, any non County-owned equipment. Personal use of County hardware or software is prohibited.
- c) If an employee finds it necessary to remove computer hardware or software (including making copies of computer programs), from their work locations, they must notify their supervisor IN WRITING prior to such removal, or be directed by the department head or supervisor in writing to do so. The written documentation shall include an estimated time in which the hardware or software will return to the County. The Department Head will maintain the written documentation for one year.
- d) This policy DOES NOT include removing off site tape or disk backups of data created and used solely for disaster recovery purposes. The Information Technology Department shall be responsible for managing all off site tape or disk backups of data.

- e) Off-site equipment shall be designated as a "floater" on the insurance inventory.

VI. Use of Non-county Software on County Equipment

- a) No software may be loaded or run on County computers UNLESS:
 - 1) Permission is granted, in writing, from a Department Head or Information Technology Department;
 - 2) The County has purchased and received the software from an authorized dealer;
 - 3) The software is an evaluation copy from an authorized dealer;
 - 4) The Department Head or Information Technology Department, or their designee, has authorized the software's use and scanned it for any viruses.
- b) Failure to comply with this policy may become grounds for dismissal or other disciplinary action. For purposes of this policy, software is defined as any program, operating system, or data files.
- c) Only software that has been purchased or leased by the County shall be considered for installation on County computers or servers.
- d) All software being considered for installation on County computers or servers must be approved by Department Heads, AND in coordination with the Information Technology Department.
- e) All software must be scanned for possible virus contamination BEFORE it is loaded on any County equipment.
- f) This policy explicitly prohibits installation of all games, shareware programs, public domain programs, and employee purchased programs, without permission from Department Head, and in coordination with the Information Technology Department.
- g) When permissible, downloading from a bulletin board service, or Internet, the downloaded files must be scanned for viruses before copying to the network.

VII. Security of Sensitive Information

- A. Any information that due to legislative mandate or other cause is defined as sensitive or confidential in nature must be kept secure. Confidential information includes any information protected by County, State, or Federal privacy acts or administrative regulations. In addition, it should include anything that in the opinion of the department head would be appropriately kept confidential in order to protect the interests of the County, its employees, or its clients, so long as such action by the department head does not conflict with relevant open meetings and records statutes.
- B. The level of security provided should be that required by statutory mandates or that which is appropriate to the sensitivity of the information. Each department head shall be responsible for developing and maintaining the appropriate security

procedures necessary to ensure compliance with confidentiality and security requirements.

Types of security include:

- 1) Limited facilities access, such as locking an office door.
- 2) Software access security to local hard disks or directories.
- 3) Local Area Networks ID, Password, and Directory security.
- 4) Logging off the network when away from workstations for lunches or breaks.
- 5) Controlled Login / Logout Time Restrictions on all Electronic Public Health Information (EPHI) computers, which complies with HIPAA 45 CFR § 164.310 (d)(2)(iii) – Automatic Log-Off Procedures
- 6) Automatic Screen Savers with password protection on all EPHI computers, which complies with HIPAA 45 CFR § 164.310 (d)(2)(iii) – Automatic Log-Off Procedures
- 7) Written Global and Local Security Policies with Windows Operating Systems

VIII. Passwords Usage Procedures

- a) All employees must use a password to access the County's Local Area Networks.
- b) All HIPAA Workforce employees must have password-protected workstations, as well as separate passwords to login on electronic protected health information (EPHI) applications. This user group must also use extra precaution with EPHI workstations, such as applying password-protected screen savers on local computers. This complies with HIPAA 45 CFR § 164.308 (a)(5)(ii)(d) – Password Management Procedures
- c) All employees must use a separate password to connect to the Internet, and web-based applications.
- d) Passwords must be at least eight (8) characters in length
- e) Passwords must be a combination of upper and lowercase letters, symbols, and numbers
- f) Passwords cannot be anyone's names or any words that could be found in dictionaries
- g) Employees are responsible to change their password three (3) times each year. Do not enter the same password more than once.
- h) Training on password management will be performed by the Information Technology Department, or during employee orientation.

IX. Backup and Recovery Procedures

- a) It shall be the responsibility of all County employees who use County computers, to store all business-related information from their computers, to the network servers. Special home directories shall be created for each user, to store such information. Personal Computers (workstations) will not be backed up, thus any information stored on the Personal Computer (workstation) may be subject to data loss or destruction.

- b) All application data, created, modified, retrieved, stored, and disposed of, shall reside on Local Area Network Servers, and shall be backed up by the Information Technology Department a daily basis. This complies with HIPAA 45 CFR § 164.310 (d)(2)(iv) – Data Backup and Storage Procedures.
- c) Each Local Area Network in the County will have one (1) full backup performed at least weekly, with incremental backups performed daily. It will be the responsibility of the Information Technology Department to perform these backups, to arrange for secure off site storage, and to develop and implement the Network backup and recovery procedures specific to their Local Area Network. In addition, the Information Technology Department will develop and maintain a complete set of documentation on their LAN following the LAN Documentation Guidelines.

X. Quality Assurance of Business Critical Information

- a) Each individual that produces reports or other information that is used to make business decisions within the County must have a process in place to verify that the information being provided is timely, accurate, and correct.
- b) It is the responsibility of each supervisor to ensure that the employees under their control have developed and are using procedures to ensure the quality of business critical information. These procedures may include: cross footing totals in spreadsheets, reasonableness checks of raw and summary data, having another individual review your spreadsheet formulae or database program, etc.

XI. Designated Key Employees

- a) Each Department Head will assign one or more "Responsible Person(s)" as liaison(s) between that department and the Information Technology Department, to communicate computer-related issues.
- b) Each Department Head, or liaison, will assign or arrange for technical support to assist in the support of some or all of the workstations in that department.
- c) The Information Technology Department's job responsibilities will include maintaining security, adding and deleting users, controlling network printing, developing and maintaining LAN documentation, performing LAN data backups and restores, assisting end users with learning and using the LAN, and trouble shooting network problems.

- d) The liaison will act as a local contact or knowledgeable person to help work with other end users in their workgroup to help support their computerized work efforts.

XII. Purchase of Hardware

- a) All Personal Computers, printers, modems, and other peripheral equipment purchased by County departments are the property of the County. In an effort to standardize equipment, all hardware must be purchased through the Information Technology Department.
- b) Each Department Head may contact the Information Technology Department directly for information regarding equipment, pricing and availability of PC's, LAN's, or peripheral equipment.
- c) Actual procuring and receiving of computer-related hardware must come through the Information Technology Department, as they will appropriately document, inventory, and distribute it to the purchaser.
- d) All computer-related hardware purchases must be coordinated with the Information Technology Department for compatibility, and adhere to the Purchasing Policy and Procedures.

XIII. Purchase of County-Owned Used / Refurbished Hardware

- a) When additional hardware is needed by departments, in the course of county business, they can request to purchase any available used / refurbished county-owned hardware from the Information Technology Department.
- b) Such used / refurbished county-owned hardware is inclusive to only laptops, computers, monitors, and laser printers. All such hardware shall be based on a five (5) year life cycle and depreciates at a rate of 20% annually.
- c) Departments can purchase this equipment at a reduced rate, depending on the age of the equipment. (An example: an \$800 computer that is 4 years old will be discounted 80%. The cost of to the department would be 20% of \$800, or \$160.)
- d) Minimum charges for purchasing county-owned used / refurbished hardware shall be 20% of original cost. All dollar amounts shall be rounded to a whole figure.
- e) In the event that county-owned used / refurbished hardware becomes defective in the same year it was purchased, the Information Technology shall be responsible only to repair such equipment as necessary, or replace such equipment with another used / refurbished hardware. If there isn't any equipment available for replacement, departments have no recourse but to purchase new.
- f) Departments that purchase any county-owned used / refurbished hardware, will be responsible for adding this hardware to their Repair / Replacement (R/R) equipment list, and budgeting for the R/R hardware fees in the next budget cycle, and beyond. In the budget cycle following the purchase of the above-mentioned hardware, any repairs or replacement costs to the above-

mentioned hardware will be covered by the R/R budget fund account, and not incurred by departments.

XIV. Purchase of Software

- a) All software purchased by the County departments is the property of the County.
- b) All software purchased by the County departments, shall only be installed on County computers, unless explicitly allowed and documented by software vendor / developer agreements.
- c) Certain software products have been selected as standard (global) and appear on the "Supported Products List" (See Appendix A: Polk County Supported Products List, below). The Information Technology Department will maintain the supported products list. All purchases of global software must receive prior approval from the Information Technology Department. Licenses and registration of global software shall be verified by the Information Technology Department.
- d) Certain software products have been selected as specific (proprietary) and appear on the "Limited Products Support List". The Information Technology Department and Department Heads will maintain duplicated copies of the limited products support list.
- e) Each Department Head, or their designees shall be responsible for researching, acquiring product information, and consulting with the Information Technology Department, prior to purchasing proprietary software.
- f) Each Department Head, or their designee shall be responsible for accurate and current Licenses and registration of proprietary software with copies of the documentation being forwarded to the Information Technology Department for record keeping and updating the Limited Products Support List.

XV. Technical Support

- a) Technical Support for all of the County's Personal Computers, Local Area Networks, and global software (on the Supported Products List) will be provided by the Information Technology Department.
- b) The Department Heads must arrange technical Support for proprietary software on the Limited Products Support List. Such support may include the assistance of the Information Technology Department, contract support vendors, product developers or technical consultants, who have been pre-approved by the governing committee or the Information Technology Department.
- c) All existing support contracts should be reviewed by, and between, the Department Heads, or their designees, and the Information Technology Department by April 15 of each year.

- d) Departmental Heads and their liaisons may contact the Information Technology Department for computer-related support. All other users should request a contact through one of these individuals for computer-related issues.
- e) All County-owned entities, which maintain their own operating budgets, are responsible for service and support to their computer-related hardware and software. Any requests for technical support from the Information Technology Department shall be fee based, and only available if county workloads allow.

XVI. Warranties

- a) All departments are responsible for out of warranty maintenance and repairs. They shall budget appropriately for maintenance and technical support on proprietary software.

Appendix A: Polk County Supported Products List

- a) Supported Products List
Operating Systems: Microsoft Windows 98 2nd Ed. and greater (Service Packs included)

Network Operating Systems: Microsoft Server 2000 and 2003 (w/ Service Packs), Novell 5.1 and greater (Service Packs included)

Word processors: Microsoft Office Suites (Service Packs included)

Spreadsheets: Microsoft Office Suites (Service Packs included)

Databases: Microsoft Office Suites (Service Packs included)

Menu Systems: N/A

Email/Scheduling: Groupwise / EXCHANGE SERVER

ANTI-VIRUS NETWORK ASSOCIATES (McAFEE), SYMANTEC

CLIENTS NOVELL, MICROSOFT, SQL, SMS, McAFEE, BORDERMANAGER, GROUPWISE, CITRIX

- b) The need for upgrades will be assessed during the annual budgeting process between Department Heads and the Information Technology Department.

Appendix B: LAN DOCUMENTATION STANDARDS OUTLINE

I. GENERAL OVERVIEW:

II. PERSONNEL INVOLVED:

- A. INFORMATION TECHNOLOGY DIRECTOR
- B. INFORMATION TECHNOLOGY SPECIALIST 1
- C. INFORMATION TECHNOLOGY SPECIALIST 2
- D. PROGRAMMER

III. LAN HARDWARE CONFIGURATION:

- A. PHYSICAL LAYOUT
 - 1. WIRING DATABASE
 - 2. LOCATION DIAGRAMS

- B. FILE SERVERS
 - 1. ATTACHED EQUIPMENT
 - 2. PHYSICAL DISK DRIVE ORGANIZATION
 - 3. LOGICAL DISK DRIVE ORGANIZATION

- C. OTHER SPECIAL WORKSTATIONS
 - 1. GATEWAY
 - 2. PRINT SERVERS
 - 3. ROUTERS
 - 4. SWITCHES
 - 5. FIREWALLS
 - 6. INTRUDER DETECTION SYSTEM

IV. SOFTWARE CONFIGURATION:

- A. NOVELL OPERATING SYSTEM

- B. LAN NETWORK & LOCAL PRINTERS

- C. FILE TRANSFER SOFTWARE

- D. PURCHASED LAN BASED SOFTWARE

- E. IN-HOUSE DEVELOPED LAN SYSTEMS

V. LAN RELATED BACKUPS:

- A. DATA
- B. SOFTWARE
- C. HARDWARE
- D. PERSONNEL

VI. RECOVERY PROCEDURES:

A. DATA LOSS/ERROR RECOVERY

B. DISASTER RECOVERY:

1. LOSS OF HARD DISK(S)
2. LOSS OF FILE SERVER
3. LOSS OF LAN
4. LOSS OF GATEWAY
5. LOSS OF BUILDING

VII. QUALITY ASSURANCE:

- A. INHOUSE DEVELOPED LAN SYSTEMS
- B. END USER CREATED INFORMATION
- C. PROGRAM CHANGE CONTROLS (LOG FILE)
- D. TESTING OF SHAREWARE FOR VIRUSES
- E. PRODUCTION CHANGE LOG

VIII. ACCESS SECURITY:

A. PHYSICAL FACILITIES ACCESS TO EQUIPMENT

B. DIALIN ACCESS FROM OUTSIDE THE BUILDING

C. LAN SOFTWARE ACCESS CONTROL SECURITY

1. LOGIN ID/PASSWORD
2. USER/GROUP TRUSTEE RIGHTS
3. FILE ATTRIBUTE LOCKS
4. STATION/TIME RESTRICTIONS

D. INHOUSE APPLICATION SECURITY AND AUTHORIZATION

X. ONGOING LAN OPERATING AND MAINT PROCEDURES:

1. ADDING/DELETING LAN USERS
2. ADDING/DELETING NETWORK PRINTERS
3. ADDING/DELETING PURCHASED SOFTWARE
4. ADDING/DELETING LAN WORKSTATIONS
5. MONITORING SYSTEM USAGE/PERFORMANCE
6. UPGRADING LAN SOFTWARE