EXHIBIT O

# Management Information Services Department Policy & Procedure Manual

MIS Department
120 W. Conant St.
Suite 101
Portage, WI 53901

# Contents

# Introduction

These policies and procedures are intended for use by the employees of the Management Information Services Department of Columbia County Wisconsin. Where more specific policies exist at a higher level (I.E. County, State or Federal) the higher level policies must take precedent.

Note: Refer to the Human Resources Personnel Manual for a complete compilation of countywide personnel policies.

# General Office

## Department Teams:

### *Management Team*

Coordinate, monitor and manage significant information technology projects across county government. Establish departmental goals based on the current and anticipated needs of the supported customers.

Each team manager is responsible for insuring that their respective teams are adequately staffed to meet the expected demands for each given work day. The personnel manual will be used to provide guidance for approval/disapproval of requested leave.

There will always be at least one manager here on normal workdays. While this does not mean that there will always be a manager in the office, it does means that the managers will coordinate their calendars to avoid the situation where both managers are out on personal leave, attending training, or some other daylong event.

### *Application Team*

Develop, maintain and support the application programs that are used by county employees. Direct maintenance support is limited to systems that are developed and maintain by the County. Purchased, or third party applications support is limited to integration and interface support.

### *Infrastructure Team*

Install, monitor and maintain the individual components that make up the collective infrastructure systems used by all county departments. This includes, but is not limited to, servers, workstations, laptops, routers, switches, wiring and software. A detailed list of individual

### *Weekly Team Meetings:*

Each team will meet weekly to review team projects and individual assignments. Project priorities and progress will be discusses as well as identifying any issues that require additional attention or support from one of the other teams.

### *Quarterly Department Meetings:*

Each calendar quarter, the MIS department head shall schedule and preside over a meeting of the department staff to review department goals/objectives. Additionally, this meeting will be used to brief the staff on issues such as security, safety and professional conduct.

# Support Hours:

## *Normal*

Normal Office Support Hours:
Monday – Friday: 8:00am – 4:30pm

## *On Call*

After Hours On Call Support Hours:
Monday-Friday 4:30pm – 8:00am,
All day Saturday, Sunday & Holiday

## *Flex Hours*

Flex Hours are allowed to meet operational requirement to cover off-hours support duties. Flex hours are coordinated with the individual MIS employee and are at the discretion of the Department Head.

## *Vacation & Comp Leave*

MIS employees must request use of vacation and compensation time in writing (email) to their immediate supervisor at least 5 days in advance. The employee's supervisor will balance the department's anticipated operational needs with other preexisting staff requests and only approve requests if the operational needs will be adequately supported.

Throughout the year, each employee would limit their accumulated compensation time to 20 hours. This will allow the employee to keep up to 20 hours of available compensation time to be earned during an unexpected emergency when overtime is required. Any compensation time earned beyond 20 hours must be taken off within the next pay period or as soon as practicable.

At the beginning of the fourth quarter of each year (October 1$^{st}$) each employee will propose a time-off schedule that will result in his/her using up all accumulated compensation time before the end of the year. The department head will approve the proposed schedule so long as it does not adversely impact the MIS Department's ability to meet mission requirements.

## *Planned Sick Leave Use*

MIS employees must request use of planned sick leave time in writing (email) to their immediate supervisor as soon as the employee is aware of the planned leave. The employee's supervisor will balance the department's anticipated operational needs with other preexisting staff requests and may need to cancel previously approved vacation leave of other employees in order to insure that the operational needs of the department will be adequately supported.

## *Employee Outlook Calendar*

All MIS employees must keep their individual outlook calendar current. Their calendar must show their normal work day scheduled and all events that will result in their being out of the office and/or unavailable.

### *Out n About Calendar*

All MIS employees must keep their individual Out n About status current whenever they are out of the office.

### *Overtime*

Outside of on call work, MIS employees must request and receive approval in writing (email) by the employee's supervisor before the employee works beyond normally scheduled hours.

During on call work that lasts for less than two hours, MIS employees must notify their immediate supervisor as soon as practicable (via email) that on call work has taken place.

During on call work that lasts, or is expected to last, for more than two hours, the employee must attempt to notify their immediate supervisor (via cell phone) as soon as possible.

### *Lunches/Breaks*

Breaks are defined in section 7.23 of the Human Resources personnel manual.

### *Bi-Weekly Timesheet*

Each employee is required to provide his or her supervisor with a biweekly timesheet for review and approval. The timesheet form is found on the MIS page of CCWeb. The timesheet must accurately record the employee's hours (regular, sick, vacation, …) during the current reporting period. The employee should contact their supervisor for assistance if they are unclear as to how to properly fill out the timesheet.

Employee timesheets are due on by the end of business day on the Thursday of every non-payday week. Supervisors must review and approve each employee's timesheet before 12:00 noon on the non-payday Friday. The processing of the timesheet information must be completed and sent to HR/Payroll by the end of business that Friday.

(Note: Changes in the work week, such as a holiday, may result in the Human Resources Department requesting a revision to the timeline listed above. Employees will be notified of any timeline changes.)

## Dress Code:

The overall style of dress during the week is as follows:

- Monday through Thursday - *business casual*

- Friday - *in-office casual*

General considerations that always apply:

- Clothing should be clean, neat, coordinated, and in good condition.
- Clothing should be appropriate for the anticipated work tasks.
- When meeting outside of the office, while representing Management Information Services, staff must dress to the standard of the hosting organization.
- When meetings are hosted by Management Information Services, staff is expected to dress appropriately to the stature of the invited guests.

For the purposes of this policy, the following definitions apply:

*Business casual*:

> "A level of dress which reflects a comfortable yet professional office environment while maintaining an appearance that is consistent and appropriate for the position, authority and task being performed by the individual."

*In-office casual*:

> "A level of dress which reflects a comfortable and casual working environment while encouraging staff to interact on an informal basis regardless of position or authority."

## Ethics

Refer to County Ordinance Title 3: Code of Ethics.

## Office Etiquette:

Below is a list of three areas of office etiquette, *courtesy, atmosphere, and safety*. Included with each area are some helpful guidelines for staff to follow to try and avoid some of the interpersonal misunderstandings that can erupt when staff works in close proximity to one another.

### *Courtesy*

MIS is an open working environment, and as such requires that staff exercise appropriate care and consideration for how individual actions can impact the ability of coworkers to do their jobs. Common courtesy items are:

- Be aware of the impact that you and your guests have on the work effort of those around you.
- Avoid making loud conversation or disruptive noises.
- Talk within the cubicle space, not over or through cubicle walls.
- Use individual headphones, with volume set to an appropriate level, to avoid disrupting others.

- Act as though you are entering someone's office when entering cubicle space, knock or announce yourself. Don't just stand behind someone hoping they will see you.
- Creating distracting noises, such as tapping, whistling, or humming should be avoided.
- Meetings, both scheduled and impromptu, should be held in the meeting rooms whenever possible.

### *Atmosphere*

The workspace, both cubicle and office, is a "semi-private" workspace. The amount of personalized touch that an individual gives to his/her cubical or office is generally up to the individual, so long as the accessories are appropriate to a professional setting.

- The general appearance of individual work space should reflect a professional working environment.
- Nothing should extend above or beyond the parameters of the cubicle or office. Decorative items may be placed atop cubicle partition storage bins if the storage bin is against a fixed wall, reducing the likelihood that the item would create a safety hazard if it fell.
- Storage bins are to be closed at the end of each work day.
- Care should be taken during visits from friends and family to minimize any disruption to other staff engaged in work.
- All employees shall practice proficient file management, keeping work and work material in good order.

### *Safety:*

Although we should always be on the alert for safety issues, it's all too easy to oversee some of the most obvious safety hazards. Some common office safety considerations include:

- Use good judgment to avoid accidents from happening in the first place
- Don't run in the office
- Don't block entrances to cubicles, offices or boxes or item in walkways which could create a tripping hazard
- Don't store items on top of storage bins which could easily fall and injure someone or damage property
- Use proper lifting technique
- In the event of an accident:
  - Take all necessary action as required to protect the safety of yourself and others (i.e. evacuate the building, call emergency services, …)
  - Report the accident to your supervisor as soon as practicable even if the accident seems to be very minor

## Computer Use:

### *Screen Savers*

**Confidential Information Accessible:** Screen saver must be set to automatically activate after 5 minutes of inactivity. Additionally, the computer must be configured

to require a password to access the computer after the screen saver has been activated.

**No Confidential Information Accessibility:** Screen savers must be set to automatically activate after 20 minutes of inactivity. Additionally, the computer must be configured to require a password to access the computer after the screen saver has been activated.

### *After Hours*

Under normal circumstances, workstations should be shut down at the end of each work day. Assigned workstations may be left on if there is the likelihood that the employee will need to remotely connect to their workstation in order to conduct county business.

### *Personal Use*

Use of county owned computer equipment for personal use is strictly forbidden. In some instances the use of a county owned computer might constitute a dual purpose to satisfy both professional and personal needs. In such cases, the employee is expected to seek supervisor approval prior to using the computer.

### *Email Use*

All email must be read and responded to in a prompt and timely manner, using proper grammar and etiquette. Spell check should be utilized to ensure accurate communications. All interdepartmental communications related to MIS Department policies or procedures must be reviewed by a supervisor before the email is sent. Use of the County's email systems is restricted to county work related activities.

## Telephone:

In general, the employee should remain vigilant in the use of the County's phone systems and always attempt to use the least costly option whenever practicable. Additionally, the employee should keep in mind that these telephone systems are public property and personal use should be kept to a minimum.

### *Office Phones*

Each employee is assigned an office telephone number as their primary county contact number. The phone must be forwarded to either another phone number or voicemail so as to avoid any unanswered call situations.

### *Cellular Phones*

Some MIS employees are assigned a cellular phone dependant on job responsibilities. The employee is required to monitor their usage and report missing/damages cell phones as soon as practicable. Personal use of a county provided cell phone is restricted to emergency use only. The employee will be held accountable if the phone is lost or damaged through neglect.

## *Voicemail*

Each employee is assigned at least one voicemail account. Outgoing messages must be professional. The employee is required to check these accounts on a regular basis throughout the normal business work day and delete old messages to avoid excessive storage on the voicemail server.

# New Employee Orientation:

## *Administrative Checklist*

Note: Also reference section 7.11 of the County's Personnel Manual.

1. Overview of the Organization
   - County Organizational Structure
   - Other

2. Department Functions
   - Department structure
   - Department objectives
   - Department activities
   - Relation with other departments
   - Other

3. Job Duties
   - Job Description
   - Performance Measures
   - Other

4. Department Policy and Procedure
   - Work schedules
   - Vacations
   - Holidays
   - Leaves of absence
   - Breaks
   - Lunch period
   - Time sheets
   - Paperwork requirements
   - Supplies
   - Transfer calls to other departments
   - Personal telephone calls and mail
   - General appearance
   - Handling confidential information
   - Other

5. Compensation – Pay Scale
   - Overtime/comptime
   - Holiday pay
   - Paydays
   - Other

6. Safety
   - Safety data sheets
   - Safety requirements
   - First aid
   - Emergency Plan
   - Incidence report
   - Other

7. Physical Facilities

- Building & Office layout
- Employee entrance
- Parking
- Cafeteria/Break Room
- Department tour and introductions
- Other

8. Relevant Federal/State Personnel Laws
   - Americans with Disabilities Act
   - Sexual Harassment/Discrimination
   - Other

9. Assigned County Property

   You will be required to turn in the following items when you leave county employment.

*County Property Checklist*

| | *Initial* |
|---|---|
| Office Keys | _____ |
| ID Card | _____ |
| Parking Sticker | _____ |
| Cell Phone | _____ |

*Signature Block*

_____ _____
Employee's Signature Date

_____ _____
Department Head Signature Date

(Department Head must photocopy signed form and retain within employee departmental records folder.)

# Separation Processing:

## *Administrative Checklist*

Prior to the employee's last work day, the department head will insure the following administrative functions are completed or scheduled:

_____ Conduct exit interview with employee
Document areas of criticism including suggested improvements.

_____ Letter of Resignation, if amicable separation
(Letter must including last day as county employee.)

_____ Verify accountability of all accumulated time
(Including vacation and compensation time.)

_____ Disable all user access accounts

_____ Transfer employee's files/documentation to alternate employee

_____ Transfer employee's responsibilities to alternate employee

_____ Change former employee known access codes

## *County Property Checklist*

Prior to the employee's last work day, the Department Head will account for the following assigned items and compare with signed county property form in employee's departmental folder:

_____ Office Keys

_____ ID Card

_____ Parking Sticker

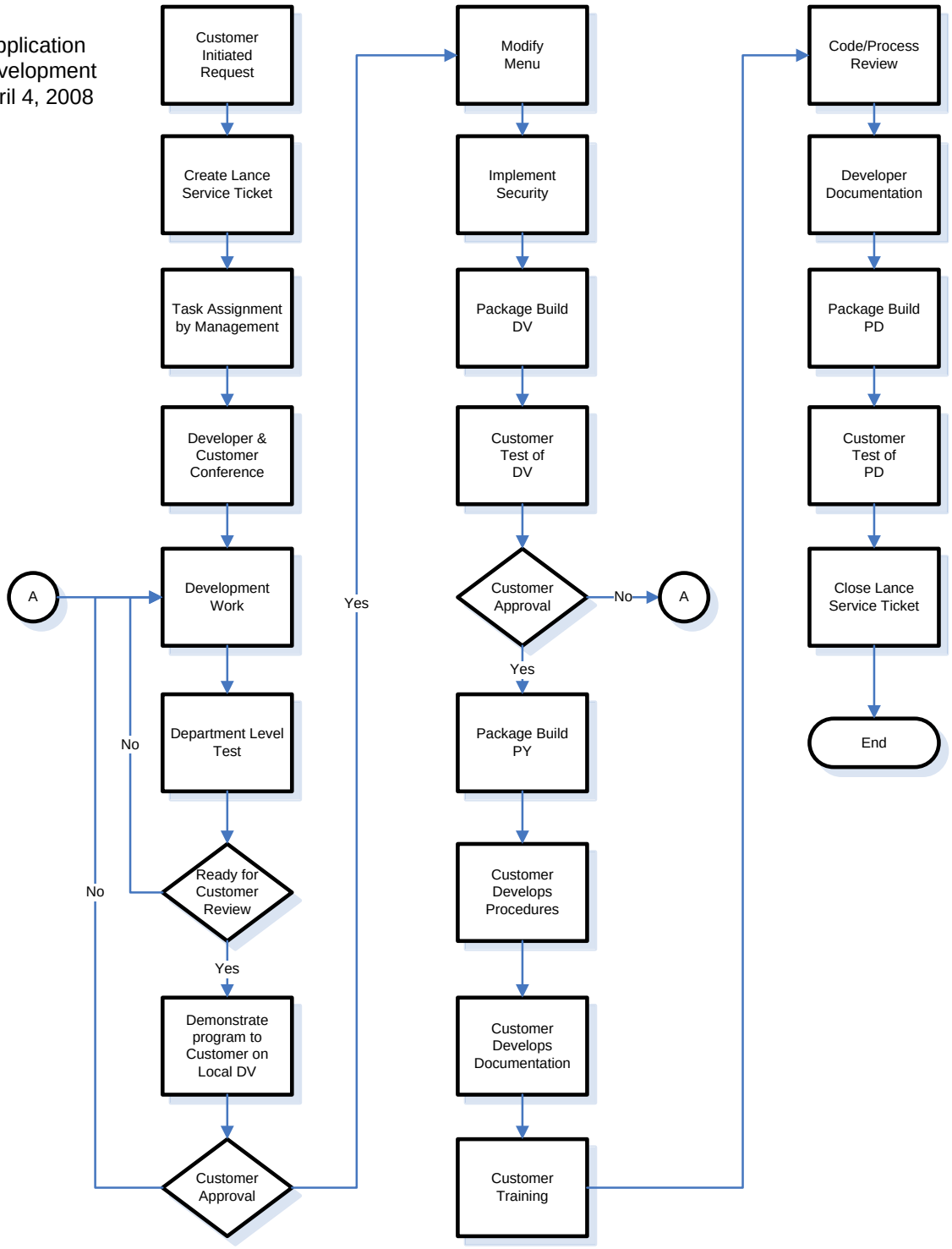
_____ Cell Phone

## *Personal Items*

Insure all personal items are removed from office/cubical work area, including all pictures, desk drawer contents and wall hangings.

## Applications Development/Support

Application Development
April 4, 2008



## MIS Committee

### *Presentations*

As the governing body for the MIS Department, employees may, from time to time, be required to present information to the Committee. These presentations are intended to provide the Committee with a better understanding of the scope of services provided by the MIS Department and the detail of how those services are provided.

## Public Interaction:

### *General*

In general, the normal MIS customers consist of other county departments and not the public. While these other departments may have direct interaction with the county citizenry, the MIS Department has only indirect contact with the public. Our success as a department is, to a large extent, determined by how effective our customers are able to meet the needs of their customers with the information tools that we provide.

### *News Media*

Only authorized personnel are to discuss topics with anyone from the news media. The only MIS personnel authorized to talk with the news media are the department Director and Applications Manager. All other staff should refer any questions to appropriate authorized individual.

# Financials

## Purchases:

All County policies regarding purchasing take precedent over MIS Department policies. The employee should check with the Accounting Department if you are in doubt as to how to a purchase request or purchase order is to be processed.

### *Purchase Requests*

At a minimum, two individuals must be involved in each purchase.
One individual will create the purchase request, the Department Head will evaluate the request and approve or reject as is appropriate.

### *Purchase Orders*

After the Accounting Department has provided a MIS copy of the purchase order, the original requester will either FAX or scan the PO and email it as an attachment to the vendor. The MIS copy of the PO is to be placed in the inbox of the MIS Department Head until the item and its corresponding invoice has been received by the department head.

## *Credit Card Purchases*

Title: MIS Department – Credit Card Use
Date: March 14, 2008

**Background:** The County has entrusted the MIS Department with the responsible use of a credit card. The user of the credit card is expected to understand and adhere to the following policy:

**Policy:**

- The use of the credit card must comply with all other county policies regarding the use of credit cards. Refer to the *Credit Card Use Policy* provided by the Accounting Department.
- The use of a normal county purchase order is the preferred method of making purchases. This card is intended to be used only when the normal purchase order process is not viable.
- Use of the credit card is permitted when the vendor will not accept a standard purchase order. An example of this might be an internet based purchase.
- Use of the credit card is permitted when the purchase time is critical and a normal purchase order process is not practicable. An example might be an after normal business hours purchase of an item to restore critical services.
- Use of the credit card is permitted when the employee is at a remote location and conducting county business. An example of this might be a rental car.
- Purchases made with the credit card must meet the definition of what can legitimately be purchased with county funds.
- Individuals requesting the use of the credit card must confirm the need with the MIS Department Head prior to use.
- Receipts for all purchases must be provided to the department head.
- When not in use, the credit card(s) must be kept under lock & key in the department head's desk.

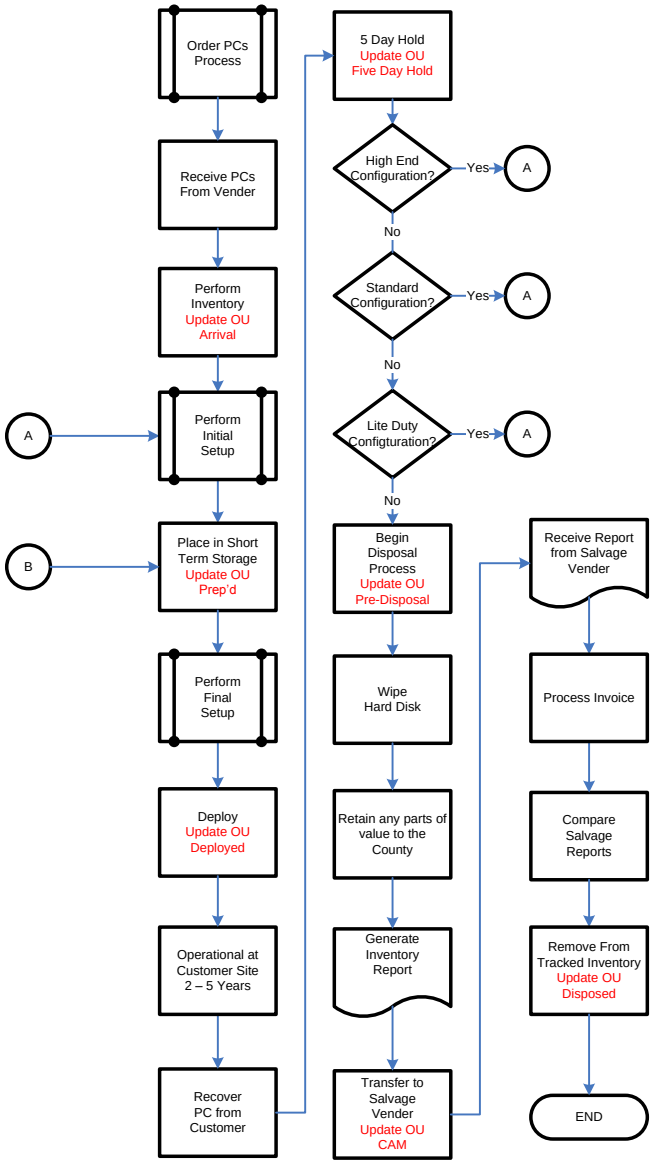
## *Receiving*

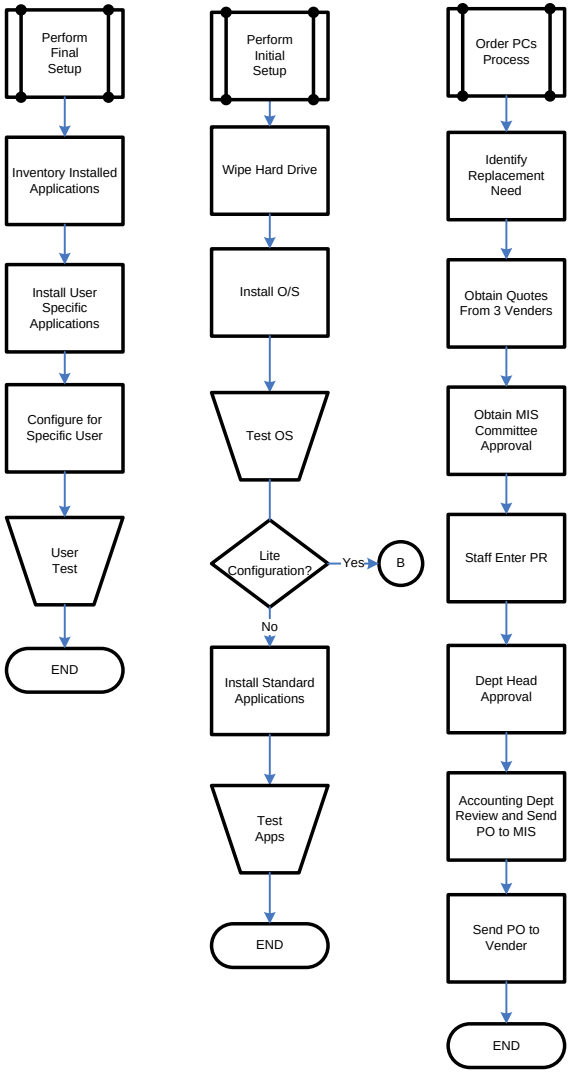
Upon delivery of any item, the receiver must insure:

- The proper delivery address.
- The correct numbers of items are being received.
- **Do not** sign receipt if items are missing or heavily damaged.

Received items are to be properly stored in a secure area. The Setup Room and Surplus Storage areas are the two designated secure storage areas.

Computer
Life Cycle
April 4, 2008



Intentionally left blank.

# Record Management

## Retention

### *County Policy:*

Refer to the County policies regarding records retention in title 4 of the County ordinances. The portion of the ordinance relating to the MIS Department is duplicated here for convenience:

*Sec. 4-1-14 Data Processing.*

*County data processing provides information technology services for departments and stores record information for departments. Record information stored electronically must be maintained pursuant to the guidelines established for the specified departmental records and County-wide records enumerated in this Chapter.*

### *Electronic Mail*

Standard record retention length for electronic mail is seven (7) years. However, each department is allowed to make its own determination based on operational and statutory requirements.

### *HIPAA Compliance*

Standard record retention length for all HIPAA related compliance documentation is six (6) years.

# Computer Maintenance Support Programs

## Inventory:

### *Department Computers:*

The Accounting Department annually provides the MIS Department a list of how many and which type of computer each department has budgeted. This list is compared with the prior year list to determine what increases or decreases of computer assets are required to keep each department in compliance to what it has budgeted.

### *Department Printers:*

Currently, department printers are the responsibility of each individual department and are not inventoried by the MIS Department.

## Computer Replacement Policy

### *Replacement Criteria*

In general, computer systems, including individual components such as monitors and hard drives, are replaced on an as needed basis and not replaced on a chronological base due to age. However, when systems and/or components begin to show signs of becoming unreliable, (i.e. regular lock ups or requires frequent rebooting) or if the device is no longer able to perform the function for which it was installed, then the device will be replaced.

### *High-End Computers*

Some systems, such as high-end CAD computers, will require regular upgrades to their processor(s) and memory in order to keep them within the bounds of the system requirements for their specialized software. It is expected that the hardware requirements for specialized software will continue to expand as the software becomes more sophisticated.

### *Computer Lifecycle*

The normal lifecycle of a computer system includes moving a computer from one use to another, which includes a gradual gravitation toward providing services that require less capability. (i.e. High-end systems become standard desktop systems, standard desktop systems become low-end systems) Consequently, a computer system may provide services on multiple levels between the time it is originally purchased and when it is finally determined to no longer be capable of fulfilling any county need and is marked for disposal.

Below is a diagram which graphically defines the total computer life cycle from purchase to disposal:

The computer maintenance support program provides a mechanism by which the PC infrastructure can be maintain to meet current and anticipated computer needs for all departments in Columbia County government.

## *Computer Equipment Recycling and Disposal*

When computer equipment is returned to the MIS Department from a customer site it must be evaluated for possible redeployment or disposal. The equipment (including individual subcomponents) is evaluated to identify any material or monetary value to any Columbia County Department operation.

NOTE: ALL PCs HARD DRIVES MUST BE WIPED USING AUTHORIZED DISK SCRUBBING SOFTWARE BEFORE THE PC IS REUSED OR SENT FOR DISPOSAL. ALL SERVER HARD DRIVES ARE TO BE PHYSICALLY DESTROYED AFTER REPLACEMENT AND VERIFICATION.

## *Evaluation Criteria:*

1. Is there any department in the county that has a pre-existing need for the computer equipment in question? If so, the equipment is to be designated to satisfy the existing need and scheduled for deployment.

2. Is there any department in the county that is expecting to have an upcoming need for the computer equipment in question? If so, the equipment is to be earmarked and designated for the anticipated need and stored until such time as it can be deployed to satisfy the need.

If neither of 1 or 2 above applies, any information stored on the equipment is destroyed using whichever means is most cost effective. The equipment is then turned over to the vendor responsible for recycling old computer equipment.

## *Computer Equipment Disposal Considerations:*

An analysis of the current condition of the equipment and comparison for fair market value is conducted.

If fair market value exceeds the anticipated cost for advertising, selling and delivery of the equipment, then an attempt to sell the equipment should be made.

If the fair market value is less that the anticipated cost for advertising, selling and delivery of the equipment, then selling the equipment should not be attempted and donation should be considered.

If a suitable recipient can be identified and if the cost for preparing and delivery of the equipment is insignificant, then the equipment should be donated.

If the cost for preparing and delivery of the equipment for donation is significant, then the equipment should be disposed of using the least costly means possible, usually through the County's Solid Waste Department.

## Printer Maintenance Support Program:

The printer maintenance support program provides a resource pool from which repairs and disposal costs are covered. This is an optional program. At the beginning of each budget process, the MIS Department will provide each department head with a list of the printers in their department that qualifies under this program. Each department head must determine if they want the printers in their department to be covered under this program.

### *Printer Repair*

Printers are repaired using the least expensive means possible. When practicable, the printer is repaired by the MIS Infrastructure Team. If staffing levels and other priorities prevent a quick repair, the printer repair will be called into the selected supporting vendor for external repair. All repair costs are paid from the Printer Maintenance Pool.

### *Printer Disposal*

Printers are disposed of using the selected disposal vendor. Cost for the printer disposal is paid from the Printer Maintenance Pool.

# Customer Support:

## *Overview:*

The primary function of the MIS Department is to provide customer support to the other departments that make up Columbia County government. If we fail to provide quality customer support, our customers will not be able to perform their jobs effectively and the county as a whole will suffer. This is why providing support is paramount to everything that this department does.

## *HelpDesk*

Customer initiated work order requests will normally be initiated through the primary help number (608.742.9626) or via email (help.desk@co.columbia.wi.us). All service requests will be processed through the online trouble tracking program (LANCE) and assigned to a primary point of contact (POC) for appropriate follow up.

Helpline calls for applications support are directed to the Applications Manager for distribution to the Applications Support Team. The Senior Applications Developer is designated as the first level of backup for application support Helpline call distribution. Should both the team Manager and Senior Applications Developer be absent, the person receiving the call should attempt to pass the information to the first available member of the Applications Support team.

Helpline calls for infrastructure support are directed to the Infrastructure Team Manager for distribution to the Infrastructure staff. The Senior Technical Support Specialist is designated as the first level of backup for infrastructure support Helpline call distribution. Should both the team Manager and Senior Technical Support Specialist be absent, the person receiving the call should attempt to pass the information to the first available member of the Infrastructure Support team.

## *Confidential Information*

Often times the work duties of staff in the MIS Department involve access to confidential information. This trusted access **DOES NOT** entitle the employee to access this information beyond what is required to perform their specific job duties. Any unauthorized access, use or dissemination of confidential information, in any format, outside of the MIS Department may result in immediate dismissal.

## *Limitations*

Under normal circumstances, no work will be performed on the hardware or software that is used by a customer without prior coordination and approval of either the primary user, the supervisor of the primary user, and/or the designated MIS point of contact within the user's department.

## *Notice*

Work to be performed will be coordinated with sufficient advanced notice to allow the customer the opportunity to adjust their work schedule to avoid a conflict between their work requirements and the required computer work.

## *Verification*

Work to be performed will be clearly identified before work is started. This will include clearly identifying objectives and a method to verify that the desired objective has been successfully met without adversely impacting other components of the system being changed. To the extent possible, the user should be included in the verification process.

## *Follow Up*

There will be at least one post implementation follow up contact with the customer to ensure that the support work performed was successful.

## *Training*

All employees are required to participate in training sessions designed to keep their technical and professional skills current in the needs and anticipated needs of the County. Additionally, employees are required to cross-trained their duties with others on their team.

## *Business Associate Contract*

All contract service providers that may have access to confidential information are required to read and sign a Confidentiality Agreement prior to being given access to such systems. See sample in appendix.

## *Department Vehicle Use*

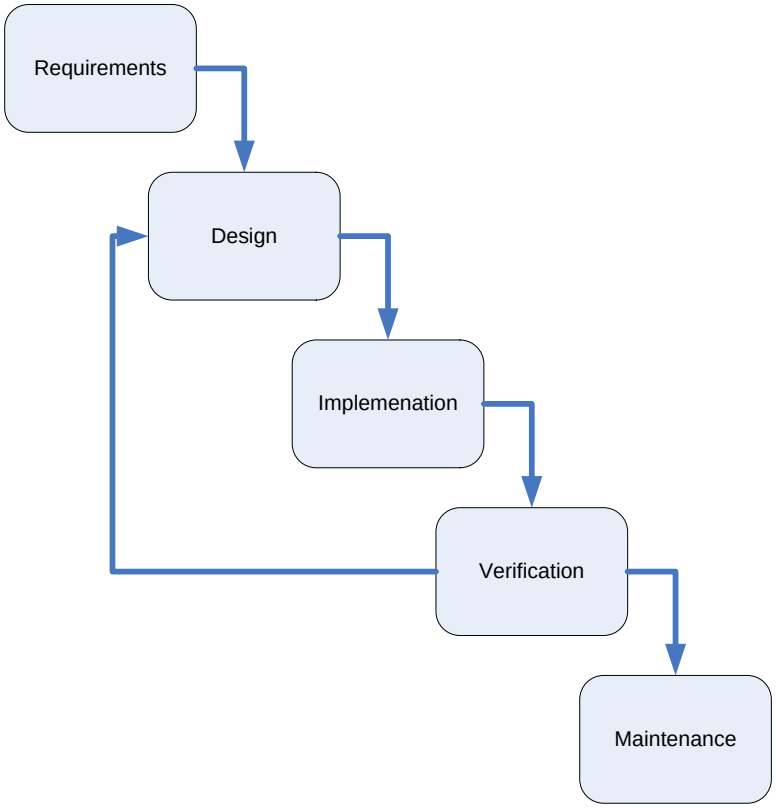
The MIS Department has a van assigned to help facilitate equipment movements and remote site visits. If moving equipment or visiting a remove customer site is required and the departmental van is not available, the employee is required to receive approval from his/her manager before they use their personally owned vehicle. Without prior approval, the employee may not be reimbursement for any personally incurred expenses.

Under no circumstances shall the van remain parked next to or near the alley behind the Annex Building after 4:30 pm. The person who last drove the van is required to move it to a more secure location (the portion of the Annex building parking lot that borders Conant Street) at the end of the work day.

The driver of the van is required to verify the fuel level is above ¼ tank at the completion of his/her use. The driver is required to refuel the van if the level is at or below ¼ tank.

# Application Development:

All application development goes through a standard set of phases. Depending on whether or not this is a new application, the complexity and criticality of the application the depth of each phase will vary. However, all application development must include all 5 phases:




## *Requirements*

Requests for new application development require several items before new application development work can begin:

- Formal Department Head request & approval will be required for any project that expends county funds.
- Lance service ticket entry will be used to track all project activity performed by the application development team and any required support staff.
- Project management entry which must clearly include the following: (Reference PMBOK file)
    - Project definition,
    - Project goals,
    - List of project stakeholders including roles & responsibilities.
    - Application Development Manager review & approval
    - MIS Department Head review & approval

Requirements phase deliverables:

- Written department head request,
- Lance Service Ticket,
- Project management file
- Requirements Document

---

## *Design*

Every project must include a dedicated design effort which clearly defines the technical parameters of the project required to successfully meet the request.
All financial application development requires a minimum of two developers to review all aspects of the program design.
Technical parameters include the following:

- Database requirements,
- Reporting requirements,
- Interfaces to other applications,
- Security considerations,
- Personally identifiable information considerations,

Design phase deliverables:

- Process Flow
- Database(s) interface(s)
- Report Inventory (new and modified)
- Documented security impacts
- HIPAA Impact Study
- Code
- Customer sign-off on design

---

## *Implementation*

All financial application implementations require a minimum of two developers to review all aspects of the program implementation.

Implementation phase deliverables:

- Change Management Analysis
- Checklist

---

## *Verification*

All financial application verification requires a minimum of two developers to review all aspects of the program verification.

Verification phase deliverables:

- Testing Responsibilities
- Test Scripts
- Test Results
- Customer sign-off on verification

---

## *Maintenance*

Text...text...

Maintenance phase deliverables:

- System Support Manual
- Training Manual
- Verify Complete Documentation
- Report Time
- Lessons Learned

---

## Application Support Process:

The Application Support Process includes the following procedures:

### *Initiate*

Must be initiated by a properly authorized individual.

### *Design*

Security, fiscal, and personal information considerations must be taken.

### *Develop*

Two sets of eyes must review all code changes for validity.

### *Test*

A separate isolated test system must be used.
Fictional data only, no production data is to be used.
Customer sign-off acknowledging the test system works as requested.

### *Implement*

Apply changes using Change Management methodologies.
Customer sign-off acknowledging the system, as implemented, works as requested.

### *Document*

Detailed description of the coding and process changes, including coders, approvers and implementers.

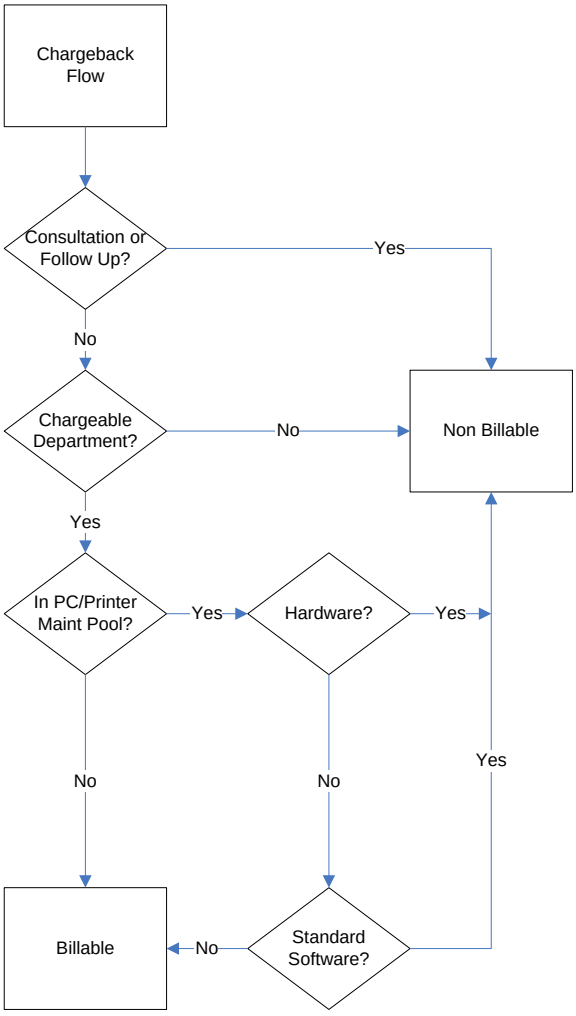
# Fees/Charges:

## *Chargeback*

Support provided to departments which can in turn chargeback to an external (non-county) agency (i.e. State, Federal, or Special Project) are charged a support fee at the standard rate as published in the budget preparation book. The Computer Maintenance and Printer Maintenance programs are not included in the chargeback process. Currently the departments that are charged back include: Highway, Health Care Center, Health & Human Services, Economic Development and Child Support Agency.

## *Decision Flowchart*

The following flowchart diagrams the decision making process to determine if the work being performed is chargeable back to the organization being helped.



# Security

## Physical Security

### *Locks*

All rooms under the control of the MIS Department must be locked when unoccupied. Additionally, the door that enters directly into the Infrastructure Team area must be locked when no Infrastructure Team members are present. Shared keys must be stored in the key cabinet located in the wiring closet within the MIS Office at the annex building.

Access to the Consolidated Server Centers, telephone PBX rooms, and wiring closets are restricted to Buildings and Grounds employees, MIS Department employees, and individuals which are escorted by MIS Department employees.

### *Cipher Locks*

Some sites are restricted using a cipher combination lock and limited to staff on a need to know basis. If a cipher lock is use, its combination must be changed after the employment termination of any individual who had access to the combination or not less than every 6 months. MIS staff are responsible for changing the cipher combination and notifying the head of the Buildings and Grounds Department after each change.

## Server Log Verification

The County uses a product called Solar Winds to record all production server logs, which includes error and warning messages.

All server logs reported on Solar Winds are reviewed at the beginning of each business day.

All errors are closely reviewed. A separate service ticket is created for each error requiring follow up action.

Warnings are reviewed and if action needs to be taken to resolve the warning message, a ticket will be created to correct it. (Some warning messages are routine and do not require follow up action.)

Brief all Infrastructure Team members of any problems/solution.

# Create New User Accounts

The following actions will be taken upon notification of new employee entering county employment:

## *Pre Employment*

5-days prior to the employee's anticipated start date: Receive completed Network New User Request Form from employee's department supervisor or department head. Form must include the full name, including middle initial, and the services required by the new employee. Employee's supervisor should identify any necessary computer or telephone training.

## *Password*

An initial password will be assigned, but will require the user to change the password on initial login. Strong password criteria are enforced. ( 8 Characters, Upper & Lower Case, Numbers and Special Characters) 90 Day forced change cycle without repeat.

On the anticipated start date, the MIS Department staff member will meet with the new employee to perform final setup of email account.

## *Authentication - CJIS*

Each person who is authorized to store, process, and/or transmit information on an FBI CJIS system shall be uniquely identified by use of a unique identifier. A unique identification shall also be required for all individuals who administer and maintain the system(s) that access CJIS data and/or networks. The unique identification will be in the form of the user's last name and badge number or the department abbreviation that they work for, followed by the first letter of the persons first, middle, and last name. These user accounts will reside in active directory.

Each user will be required to identify themselves uniquely before the user is allowed to perform any actions on the system.

Columbia County IT shall ensure that all user IDs belong only to currently authorized users, and each new account or any account to be removed from active directory will require a network user and network removal form be filled out.

## *Advanced Authentication - CJIS*

Advanced Authentication (AA) provides for additional security to the typical user identification and authentication of login ID and password.

1. Columbia County Sheriff's office and municipalities that use Columbia Counties network to access CJIS information will be required to use two-part authentication. Two-part authentication is something you know and something you have.
2. RSA Security keyfabs will be issued to each person who will be accessing CJIS information via a wireless connection in their vehicles

3. Each user will be assigned a keyfab which is assigned for their use only. No sharing of RSA Keyfabs will be allowed.
4. When accessing the CJIS system via a wireless connection, the user will need to log onto the domain using their unique userid which is assigned thru Active Directory. The user will then be required to enter in their RSA username, RSA pin and then the RSA Token key.
5. In the event that the user mistypes any of their logon credentials needed to assess the system more than 3 times, the RSA Account will be locked out, and the user will not be able to access the system
6. Once a RSA Account has been locked out, the user's supervisor must call MIS and identify themselves, and also identify the user that is locked out before a RSA account will be reset.
7. In the event a RSA token has been lost or damaged, the user must contact the MIS department to have the RSA token disabled.
8. In the event that the user is no longer working for the department, the supervisor must contact MIS and a network user removal form will be required in order to have the accounts removed and the RSA Token key must be turned back over to MIS. MIS will then deactivate the RSA Keyfab.
9. In the event that the keyfabs is owned by a municipality, the municipality must contact MIS whenever a user is no longer working for the municipality. The municipality must fill out a network user removal form. The user's accounts will be removed and the keyfab will be deactivated. Once the position has been filled, the municipality must fill out a Network user request form for the new user. The MIS department will then create the accounts( network and RSA) and assign the keyfab to the new user

## Disable / Eliminate User Accounts

The following actions will be taken upon notification of employee separation from county employment:

### *Pre Separation*

5-days prior to employee separation: Receive notice from employee's department of imminent separation of employment.

1-day prior to employee separation: Identify all systems on which the employee had been granted an account.

### *Post Separation*

Day of Separation: The user accounts will be deactivated on the date of employee separation from the county. (Note: If the employee has already separated from county employment, accounts are to be deactivated immediately.)

7-days after separation: Review identified systems for stored user account specific data.

14-days after separation: If step 2 above has not been completed, send notification (see attached template paragraph) to former employee Supervisor, copy to Department Head.

30-days after separation: Working with the former employee Supervisor or Department Head, coordinate the transfer or elimination of all data stored under the former employee's accounts.

## File Access Rights

### *Overview:*

This standard operating procedure is intended to define the conditions under which appropriately authorized individuals will be granted access to documents stored on individually assigned computers or in assigned computer accounts. These documents may include, but are not limited to, email messages, word processing documents, databases, photographs, scanned images, and other stored computer materials.

### *Conditions:*

This policy does not pertain to personnel or medical records. Access to those records is governed through Sec. 7.21 of the Columbia County Personnel Policies and Procedures Manual

All information stored on County owned computer systems are the property of Columbia County. This information may fall under Wisconsin's open record law and may be viewable by the general public. The employee should not expect any privacy with regard to documents stored on their assigned computer or data accounts.

### *Policy:*

Under normal circumstances, only the individual assigned to the data account can provide approval authority for granting access to information stored under their assigned accounts.

If the assigned individual cannot provide approval, access may be obtained from someone in the individual's higher supervisory chain.

Under exceptional circumstances, if neither the individual nor their supervisory chain can provide approval authority, access may be granted through the County's Human Resources Director and/or Corporation Counsel.

### *Open Records Requests*

All open records request received by the MIS Department are to be referred to the County's Corporation Counsel's Office for action. The MIS Department will only respond to Open Records Requests that come from the County's Corporation Counsel's Office. The MIS Director and Corporation Counsel will jointly determine the information type, quantity and detail to be provided.

# Web Use Monitoring:

## *Internal Requests (County Initiated)*

Requests for reports on a specific department's internet use will only be accepted from department heads, or individuals acting in the capacity of a department head. Up to once every three months.

Requests that are employee specific and are intended to report on the activity of a specific county employee will only be accommodated with prior approval of the County's Corporation Counsel and Human Resources Director.

## *Non-Requested/Observed Activity*

Following an observation of activity that appears to violate established county policy for internet use, the MIS Department will attempt to correct the problem through consultation with either the individual employee and/or their department head.

If attempts to resolve the issue with the employee and/or their department head are unsuccessful, the MIS Department is authorized to electronically detach the individual computer from the network and schedule a review of the incident during the next scheduled MIS Committee Meeting. The individual, their department head, the Corporation Counsel and Human Resources Director will be invited to attend the MIS Committee meeting for the review process.

# Remote Network Access:

Title: Data Network - Remote Access
Date: February 8, 2008

Accessing the County's data network from remote locations require additional security considerations. The following restrictions apply:

## *Level 1 Access Requirements*

Non Confidential Data: This level of access will allow the employee to access the county's email and intranet servers.

1. Department Head approval.

2. The creation of a level 1 remote access account.

3. Access the network using a trusted PC, such as a home computer with appropriate antivirus software.

## *Level 2 Access Requirements*

Confidential Data: This level of access will allow the employee to access county applications and stored data.

1. Department Head approval.

2. The creation of a level 2 remote access account.

3. Electronic files must be treated with the same level of care and consideration as you would apply to paper files. Any departmental policies regarding the handling of confident information, which are more restrictive, also apply.

4. The use of portable storage devices for storing or transporting confidential information is prohibited. This includes devices such as: floppy diskettes, CDs, portable hard drives, memory sticks and USB flash memory drives.

5. Use VPN (Virtual Private Network) software on a county owned laptop with up to date antivirus and patched operating system software.

6. If it is absolutely necessary to take confidential information to a remote location, the follow additional restrictions apply:

    a. Store all confidential data in an encrypted folder.
    b. When not in use, store the laptop in a secure location with the provided combination lock.
    c. Immediately report any lost or stolen materials to the MIS Department and the department responsible for the source data.

# Data Backup & Restore:

## *Policy:*

Title: Data Backup & Restore
Date: April 11, 2008

***Backup Schedule:***

- Full backups (The backing up of all of the stored data regardless of when it had last been backed up.) on all production servers occur at least once per week.
- Incremental backups (The backing up of data that has been changed since the prior full backup.) occur every work day night when full backups do not take place.
- Special needs backups occur at the request of each department. These backups will be retained for extended periods of time as determined by the requesting department.

***Additional Considerations:***

- The primary purpose for backing up server data is to allow for the full recovery of the server in the event of an equipment failure on the server. It is NOT intended for the purpose of maintaining a data archive.
- Backups must occur directly to off-site locations. (Noted exception: Due to its remote location, the Solid Waste Department performs tape backups which are manually moved off-site and stored in the MIS Department.)
- At least two full weeks of backed up data must be retained.
- Backups of confidential information must be password protected and encrypted.
- Database transaction logs are backed up at 2 hour intervals.

## *Procedures:*

Backup processes are verified at the beginning of each business day.

1. Check all backup servers for daily completion of backups. This includes incremental during the week and full backups on Fridays. Especially note the relative size of consecutive backups, as they generally are close to the same size. Large discrepancies indicate further investigation as to the cause.
2. Run the Restore function on each backup server to verify availability of restore files. There should be one full and consecutive incremental file for at least a week of potential restores. If not, manually trigger a full backup

to maintain the restore capability. When finished checking the restore potential, cancel the restore.

3. If manually triggered backups were required, monitor their progress to completion. Then verify availability of restore files.

4. Notify MIS Management and Infrastructure Team members if normal backup processes have not taken place and identify any weaknesses in the availability to recover production data.

# Software/Firmware Patch Management:

## *Definition*

All workstations, laptops, servers and network switches will occasionally require update patches to their software and firmware. This policy/procedure defines the intent and process to perform these updates.

The patches must be considered in terms of critical and non-critical. Critical patches are software/firmware updates that if left unapplied would pose a serious security or operational risk to the organization. Non-critical patches are intended to address routine features, such as usability.

## *Policy*

Regular reviews of what patches have been released by the Original Equipment Manufacturer (OEM) since the last time the equipment was updated are required at regular intervals. Critical patches must be applied ASAP. Non-critical patches are to be applied during the next normal patch update cycle.
Listed below are the defined intervals:

All workstations, including laptops, must be reviewed for operating system patches not less than one per month. All relevant patches must be applied. When possible, these systems should be configured to automatically perform this update process.

All servers (excluding appliance servers) must be reviewed for operating system patches not less than once per month. All relevant patches must be applied.

All appliance servers must be reviewed for operating system patches not less than once every three months. All relevant patches must be applied.

All network switches must be reviewed for firmware patches not less than once every three months. All relevant patches must be applied.

## *Procedure*

The initiation of each patch review/implementation cycle must be preceded by a Lance service ticket prompting the action and assigning the technician to perform the action. All subsequent actions taken to fulfill patch cycle requirement must be logged as tasks in the corresponding Lance ticket.

Each patch must be tested in a separate test environment prior to applying the patch in the production environment.

Workstation patches should be applied automatically and setup to occur at 12:00 noon on a normal workday, when the workstation is most likely to be on and available for the patch to be applied.

# Appendices

## Confidentiality Agreement

In the course of providing technical support to the computer systems used by individuals in the various departments of Columbia County, I may come into contact with information which may be highly confidential. While it is not my responsibility to determine which information is or is not confidential, I will treat all information as confidential until otherwise instructed by an authorized person.

All information regarding any County business (whether it be patient, client, staff, interdepartmental communications, associated or any other matter) must be regarded as confidential. All records including but not limited to such things as a patient's medical records, telephone conversations, family history, diseases or illnesses, County finances, and other matters must never be communicated beyond the scope of professional and para-professional personnel who require such information.

Information regarding the practice, policies, type of cases, internal problems, etc., should not be discussed with other employees, family members, personnel of other organizations, news media, or the general public except by those individuals who are directed to communicate such information at the appropriate times.

This policy concerning confidentiality shall emphasize that any infringement will be considered a violation of the rules and may lead to immediate termination.

I have read, understand and agree to the above restrictions.

_____ _____
Signature Date

_____
Printed Name

_____
Organization

(Note: Store a signed copy for each employee within their department's personnel file.)

# Routine Procedures

Telephones:

| Code | Frequency | Task |
|---|---|---|
| TEL01 | Qtrly | Review cellular usage with provider, adjust plans as warranted. |
| ~~TEL02~~ | | Not currently in use. |
| TEL03 | Qtrly | Verify voicemail hardware is functioning correctly.<br>Report problems to vendor as needed.<br>Adjust date/time as needed.<br>Verify employee list of assigned voicemail mailboxes with list of valid employees through HR.<br>Review voicemail mailboxes; notify users with > 99 messages. (Admin, HCC & HHS only) |
| ~~TEL04~~ | | Not currently in use. |
| ~~TEL05~~ | | Not currently in use. |
| TEL06 | Bi-Annual | Verify telephone employee list of assigned phone numbers. (Admin, HCC & HHS) |
| TEL07 | Qtrly | Verify telephone system hardware, report problems to vendor as needed. (Admin, HCC & HHS) |

Services:

| Code | Frequency | Task |
|---|---|---|
| SVC01 | Qtrly | Verify anti-virus software updates are occurring as intended. |
| SVC02 | Bi-Annual | Verify system & email accounts with valid employee list through HR. |
| SVC03 | Qtrly | Review available JD Edwards security updates and apply those which are warranted. (Including end of year updates.) |
| ~~SVC04~~ | | Not currently in use. |
| SVC05 | Qtrly | Reset web filtering to clear logs. |
| SVC06 | Qtrly | Update all county laptops with current software versions and patches. |
| SVC07 | Bi-Annual | Verify all financial system accounts are valid. Share account list with Accounting Department management. |
| ~~SVC08~~ | | Not currently in use. |
| SVC09 | Annual | Review Computer Hardware Asset Inventory & Tracking<br>Update documentation since last annual inventory. |

Miscellaneous:

| Code | Frequency | Task |
|---|---|---|
| MSC01 | Qtrly | Oil Shredder.<br>Change disposable bag as needed. |
| MSC02 | Bi-Annual | Review photocopier & printer logs; identify abnormalities for follow up. |
| MSC03 | Annual | Change cipher lock combination at all IT nfrastructure locations. |

Documentation:

| Code | Frequency | Task |
|---|---|---|
| DOC01 | Qtrly | Update IT Strategic Plan |
| DOC02 | Bi-Annual | Update disaster recovery plan |
| DOC03 | Annual | Review Standard Software Installation documentation and update software appendix with current tested and approved versions. |

# Standard Software Suite

| Category | Product Name |
|---|---|
| | |
| Operating System | Windows 7 Professional |
| Antivirus/Antispam | Symantec Norton Anti-virus |
| Remote Support Client | Bomgar |
| Office Productivity Suite | Office 2007 Professional Plus |
| File Server Client | File/Print Server Client 2008 (CAL) |
| Email Client | Exchange 2007 (CAL) |
| Sql Client | SQL 2008 (CAL) |
| Internet Browser | Internet Explorer v7 |
| Pdf Reader | Adobe Reader v9 |
| Burner | Nero (as needed) |
| Email Archive | Unlimited Mailbox |
| Other | Symantec Ghost |
| Other | Java v6 |
| | |
| | |
| | |
| | |
| | |

# Infrastructure Team Assignments

| ***Functional Area*** | ***Team*** |
|---|---|

**Active Directory Administration** — **Dave/Bev**

- Active directory configuration
- Domain Controller Monitor/Maintenance
- Group Policy Administration
- Login script administration
- File and Print services
- User Accounts & Permissions
- Web Servers

**Administrative** — **John/Matt/Bev**

- Policy/Procedures
- DR Planning/Testing
- Data Filtering/Monitoring

**Data and VOIP Network Infrastructure** — **Matt/Dave**

- All Switches, Routers and Wireless APs
- Wireless Campus Connections
- ASA Firewall Configuration
- VLAN Management (including QoS)
- IP Management (DNS, DHCP, WINS, etc..)
- DMZ Setup and management
- Remote Access administration (VPN and other remote access methods)
- ISP services (Charter and DSL Connections utilized by SWD and HWY)
- Public IP space
- BadgerNet Services (HOD)
- Interfaces (including video conferencing)

**Client Administration (Excluding LEC)** — **Terra/Dave**

- Standard Desktop Applications
- Ghost image administration
- Windows updates

**eSecurity** — **Dave/Matt**

- Spam Protection
- Virus Protection
- Malware Protection
- Advise Security Officer as needed.

**Hardware** **Terra/Dave**

- PCs (order/configure/maintain/inventory/dispose)
- Servers (order/configure/maintain/inventory/dispose)
- Printers & Scanners (order/configure/maintain/disposal)
- Defibrillator (battery replacement & SW updates)
- Election Equipment
- Wiring (installation & testing)
- UPS (battery test & replacement)

**Imaging** **Terra/Matt**

- ImageNow
- ImageTek
- OCR

**JD Edwards CNC** **Matt/Bev**

- Package management
- Software Management for updates
- Server Hardware Maintenance
- Application troubleshooting
- Payroll (Gneil and Kronos)

**VMware Servers** **Matt/Bev**

- Server Hardware Maintenance
- Software maintenance
- VM infrastructure management
- VM server builds & Configurations
- SAN Monitor/Management

**Communications Management** **Dave/Matt/Terra**

- Exchange server management
- Email Archiving
- Mobile phone messaging (windows, blackberry)
- Skype
- Land line phone systems (HHS, Admin/Annex, HCC, Sheriff)
- Voicemail (HHS, Admin/Annex, HCC)
- Cell Phone administration

**SQL Server** **Bev/Matt**

- SQL DBs
    - ECS
    - ESRI
    - Fidlar

**System backup and disaster recovery** **Dave/Terra**

- Routine server backups (Windows and BE)
- Network device backups (Switches, routers, APs, etc…)
- Restores

**Sheriff Client Administration** **Bev/Terra**

- Standard Desktop Applications
- Sheriff Specific Applications
- Windows Updates
- Desktop configurations

**Visonair** **Bev/Terra**

- Visionair specific applications
- Visionair integrated applications

# On Call – Technical Support Contact Procedure

Use the steps listed below to contact MIS technical support in case of a critical computer problem and the situation meets all of the following criteria:

**Criteria:**

- It is outside of normal business hours (Monday through Friday, 8:00 am – 4:30 pm).
- The problem prevents key operational functions from taking place.
- Alternate computer equipment is not available.

**Step 1**: Attempt to contact the primary on-call technician at his/her on-call cell number. (Refer to the MIS On-Call calendar.) If routed to voicemail, leave a message and wait at least 15 minutes for a technician to reply.

**Step 2**: If step 1 was unsuccessful, attempt to contact the on-call technician at his/her alternate number which is posted in the On-Call Calendar. If routed to voicemail, leave a message and proceed to step 3.

**Step 3**: If steps 1 & 2 were unsuccessful, attempt to contact the MIS Department Director. (John Hartman @ 608-697-6375) If routed to voicemail, leave a message and proceed to step 4.

**Step 4**: If steps 1, 2 & 3 were unsuccessful, attempt to contact the normal business day primary contact for the Sheriff's Office. (Bev Enke @ 608-697-7139)