Information System Security

General Information

To our customers:

At this time and for the past several months, the Division of Legislative Audit has been performing Information Systems audits around the state.

I would like to address several issues from the audits here. My intention is that these will provide you with enough background information to assist you in:

1. **Drawing reasonable conclusions from what the auditors say.**
2. **Being able to provide answers for some of the auditors' questions.**
3. **Having a good understanding of how AIS can assist your office.**

Here are some of the issues –

- **Cryptic passwords.** Made up of numbers and letters, at least 8 characters long, containing no information that relates to the user (IE: Name of a relative or pet).
  - *We have provided this type of security only in counties which request it. It is somewhat more cumbersome and most counties have not felt the need. If you wish to have cryptic passwords set up on your network, please circle this paragraph. If not, please mark through this paragraph with an "X."*
- **Forced periodic password changes**. Every 30 to 90 days, each user has to come up with a new cryptic password as described above.
  - We have avoided this in the past because it produces frustration in the users when they forget their new password. Then we get a support call to clear their password so that they can create another new one. *If you wish to have forced password changes, please circle this paragraph. If not, please mark through this paragraph with an "X."*
- **Lockout after unsuccessful attempts to log in or after a period of inactivity.** This would prevent a user from logging in with the right password after he/she tries and fails a certain number of times with the wrong password. It will also automatically lock a user out if no interaction with the keyboard or mouse occurs for a specified period of time. A password is required to re-access the computer.
  - *The login lockout feature is activated for some counties and not for others. If you wish to have the failed login lockout please circle this paragraph. If not, please mark through this paragraph with an "X."*
  - *The inactivity lockout can be applied to all workstations with Windows XP or higher. Windows '95 and '98 can provide this capability in a crude form, but frequently interrupts any process which may be running on your machine, sometimes causing it to*

900 N Dixieland Rd
Rogers, Arkansas 72756

Phone: 479.631.8054
Fax: 479.631.9291

"crash." If you wish to have the inactivity lockout please circle this paragraph. If not, please mark through this paragraph with an "X."

- **Passwords stored on the system in "clear text" form.** This means that there is a file on your system which contains user names and passwords.
  - *We have initiated a practice of removing passwords from these files. They are not used by our system and frequently are out of date anyway. When our support staff is either on site or dialed in, we will remove the "clear text" passwords from your system. If you wish to have this done on an expedited basis please circle this paragraph. If not, please mark through this paragraph with an "X."*
- **Application security restrictions can be circumvented.** This means that in some cases, a customer might be able to use Microsoft Excel, or Access to load and modify the files that our program uses. This would allow changes that our software would not allow.
  - *We are addressing this in two ways:*
    1. *Our upcoming Windows applications store data in an entirely different way and are not susceptible to this type of access.*
    2. *We can "lock down" your Windows desktop. This entails our placing more powerful controls on what you can "see" from your computer and what changes you can make in the way it performs. Some side effects of this include preventing users from having their own desktop themes, backgrounds, screen savers, etc. and preventing users from running other programs on their computer unless they are installed by an authorized administrator. IE: Calendar creator, Quicken, etc. If you wish for us to increase the level of desktop security, please circle this paragraph. If not, please mark through this paragraph with an "X."*
- **Excessive number of users with Administrative rights.** This means that in the opinion of the auditor, too many employees can access the higher level features of the program. These features may include things like voiding receipts, changing parcel numbers, recalculating the database, etc.
  - *By using the term "administrator" the auditor may be inferring privileges which in fact do not exist. An administrator for example can add or change logins, passwords, and other network settings. None of these abilities are included in the access level that the auditor observes in what he calls the "security master."*
  - *Administrative rights in our systems are mostly reserved to AIS technicians. That is why you call us when a new employee needs to be added to the system.*
  - *Our upcoming Windows based programs will have a broader and more detailed security régime which will allow finer allocation of tasks within the program itself. On the administration side, we expect to continue providing the administrative service to you unless you tell us otherwise.*
    - *If you wish to have the access privileges of your staff changed, please circle this paragraph. If not, please mark through this paragraph with an "X."*
- **Multiple users sharing a common user name and ID**. Our programs keep audit logs of significant tasks performed with the program. If everyone uses the same login, the auditors can not tell who did what.
    - *If your office has this practice, it would be best to have a separate user name and login for each employee. If you need advice or assistance in setting up your logins, please circle this paragraph. If not, please mark through this paragraph with an "X."*

Apprentice Information Systems, Inc.

900 N Dixieland Rd
Rogers, Arkansas 72756

Phone: 479.631.8054
Fax: 479.631.9291

- **Data integrity controls are inadequate.** The auditor will perform various "common sense" type checks by trying to enter data that is invalid. He might try to enter a date from 1904 instead of 2004 to see if the system will accept it. If it does, he will consider that a flaw in the program.
    - *These are not all cut and dry. For example in a recent audit the auditor wrote: "System will accept any claim number regardless of whether it has been used or not." In this case, our program had prevented this type of entry for years until 2003, when the user group asked us to change it, which of course we did. The users had a specific reason for asking this and we will honor the requests of the customer first.*
    - *As we continue to develop our upcoming Windows programs, we will incorporate as much data integrity as possible. We will do this without coming back to our customers and asking for extra funds to pay for it. If the Auditors come up with funding, we can go back and add these items to the older programs. Of course we would need some written standards to work with which appear not to exist at this time.*
    - *If you have data integrity issues that you want us to take action on, please circle this paragraph and list them on an attached sheet. If not, please mark through this paragraph with an "X."*

- **Application controls are inadequate.** Source code is the detailed programming that we create to build your programs. It is the intellectual property of the software developer. The IS audit suggests that if our company went out of business, the counties would be in jeopardy because they don't have source code. Initially Audit asked that we give them copies of the source code. Now they are asking that we put it in escrow where it could be "…released to the county…."
    - *While we believe that source code escrow is of limited value, we do offer a source code agreement to our customers so that they can gain compliance on this issue. Please contact our office for more details.*

- **No Disaster Recovery or Business Continuity plans.** This means that the County has not created and tested a written plan to continue doing computerized business in the event of a disaster such as a flood or courthouse fire.
    - *The plan itself should be developed for the entire courthouse, but this is what you can expect from AIS in case your county (God forbid) has a disaster that disables or destroys your computer system.*
        - *We will be able to provide computers and file server equipment on short notice. Our history for this is usually one business day.*
        - *We can restore your data from the nightly backup. It will be best if you are applying our recommended practice of taking the most recent tape off site each day. This tape would not likely be destroyed by the same calamity that befell the courthouse.*
        - *If you are on our backup validation program, we will have data from your system that is less than one month old. Reconstructing one month's data will be your worst case scenario.*
        - *If you are on the backup validation program, your backup system is being tested every month to assure that it is functioning properly. This will fit into the "has disaster recovery plan been tested?" question that the auditors will ask.*

In all cases where AIS is your source for network and system management, we have provided a level of security consistent with the customer's wishes. We will continue to be responsive to the customer's wishes.

Apprentice Information Systems, Inc.

900 N Dixieland Rd
Rogers, Arkansas 72756

Phone: 479.631.8054
Fax: 479.631.9291

If you have additional questions or requests related to the IS audit, please write them in the space below and then follow the directions at the bottom of this page.

Please mark the foregoing paragraphs to reflect your preferences and concerns in this regard. Then sign and return this fax to us so that we can prioritize and apply any changes that you desire.

County / Office Signature Date

Thank you for taking the time to study and respond to this survey. We take this matter very seriously and want to provide the service and programs that best meet your needs.