

Prepared for: _____ Date: _____

Completed by: _____

POLICY DEVELOPMENT

Has an appropriate person been assigned responsibility for overseeing all the company's data processing activity?

Have policies been established on the care and handling of the micro-computer and related hardware and software, including:

- a. Prohibition of eating, drinking, and smoking in the area around the microcomputer?
- b. Detailed diskette handling procedures?
- c. Periodic cleaning of diskette read/write heads?

Is use of the microcomputer restricted to employees performing assigned duties, and is use for games or other personal uses prohibited?

Have employees been warned about the company's potential liability for illegal copying of purchased software and has such copying been prohibited?

Is all computer hardware tagged with identification numbers?

Are periodic (at least annual) inventories performed of computer hardware and software?

If records of assets are maintained on the microcomputer, are employees with access to the microcomputer denied access to those assets?

Are surge protectors used?

TRAINING & DOCUMENTATION

Are two or more people (including all users) trained in the use of all hardware and each software package?

YES	NO	N/A	COMMENTS

ACQUISITION OF HARDWARE AND SOFTWARE

Are all requests funneled through one person who coordinates compatibility, negotiation with vendors, etc.?

Is a cost-benefit analysis required before acquisition so that equipment meets specific needs rather than simply a desire to have the latest equipment?

Has a clear written policy been established on the acquisition of software?

- a. Does it require compatibility so that everyone uses the same spreadsheet or word processing software?
- b. Are all requests directed to one person who coordinates compatibility, negotiates with vendors, and avoids purchasing software packages with redundant capabilities?
- c. Does a written policy exist that requires the purchase of a valid licensed copy in order to use the software on company hardware, and is there proof of the license on file?
- d. Is each software package installed only on the appropriate number of workstations?

Is all acquired software (original diskettes or CD-ROMs) tested before being used for normal processing?

SOFTWARE MAINTENANCE AND DOCUMENTATION

For all significant applications, is the following testing conducted and documentation prepared and stored in a secure location:

- a. Formulas printed out and reviewed by someone other than the developer before use?
- b. Saved and filed?
- c. Designed with an “assumptions” area to minimize changes to formulas as information is changed?
- d. Overview of functions and processing?
- e. Definitions of fields on data file?
- f. Identification of programs and their tasks?
- g. Copies of screen and report formats?
- h. User instructions, including data entry requirements, sample

YES	NO	N/A	COMMENTS

- source documents, and error message explanations?
 - i. Recovery instructions?
- Are all users aware of the effect of computer viruses?
- a. Are users aware of ways to prevent or reduce the damage caused by a virus?
 - b. Has virus protection software been installed on all computers?

PLANT SECURITY

- Are the microcomputer and related hardware physically secure?
- a. Are they in a room that is locked when the microcomputer is not in use?
 - b. If not in a locked room, is the microcomputer bolted or chained down and the cover of the processing unit locked?
 - c. Are workstations positioned away from windows to discourage theft?
 - d. Is the movement of workstations properly monitored and appropriate documentation maintained?

Are individuals authorized to use the microcomputer identified, and is the policy to challenge use by anyone else clear?

Is the microcomputer located in a place that permits management supervision?

Are diskettes stored in a secure (locked) location?

Are passwords used to the extent possible to limit access to software and files?

- a. Has the availability of optional password or encryption software been investigated and evaluated?
- b. Are existing password capabilities used effectively?

BACKUP AND RECOVERY

Are software and files backed up (copied) regularly, including the following:

- a. Operating system?
- b. Application software?

YES	NO	N/A	COMMENTS

c. Data files (master files and transaction data)?

Are backup files clearly labeled and stored separately from regular files?

CONTINGENCY PLANNING

Has a list been compiled of whom to call when a particular type of problem occurs:

- a. Repair/Maintenance service
- b. Vendors for equipment replacement?
- c. Software vendors?
- d. Location with similar or same equipment?

Has a backup location with similar equipment been identified for emergency processing? Possibilities would include the following:

- a. Other microcomputers within the company.
- b. A neighboring company or fellow user group member.
- c. Computer vendor or store.
- d. Service center

Is insurance coverage adequate for equipment, software, and costs to recover from a disaster?

YES	NO	N/A	COMMENTS