Section 6: Computer Information Systems (Continued)

J. Maintenance		
1. Are individual hardware components covered under a preventive maintenance schedule?		
2. Are maintenance procedures documented, distributed to all users and periodically checked for compliance?		
3. Are sign-off logs used in connection with equipment cleaning and operator maintenance functions?		
4. Are disk and magnetic tape drive read/write heads periodically cleaned?		
5. Is equipment such as high-speed printers and optical readers kept clean by regular vacuuming and other care?		
6. Are computer work areas kept clean and free from excessive dust and smoke?		
7. Has a policy been established prohibiting eating/drinking while working at a computer?		
8. Are components covered when not in use (to protect from dust, sprinkler systems, etc.)?		
9. Are disk drives closed or covered with a protective shield when not in use?		
10. In high traffic environments, are keyboards protected by a plastic cover?		
11. Are diskettes properly stored: 　a.　Away from extreme heat or cold? 　b.　Protected from dust, etc.? 　c.　In protective envelopes? 　d.　Away from water or excessive moisture? 　e.　Away from all magnetic devices including radios? 　f.　Upright?		
12. Are service contracts obtained for possible major repairs?		
13. Is the hard disk drive reviewed periodically with unneeded files deleted or removed to a backup CD?		
14. Is CPU usage being monitored and tracked?		
Additional Questions/Explanations:		

Section 6: Computer Information Systems (Continued)

K. Backup		
1. Are proper daily/weekly file backup and retention procedures in place, and are they being properly adhered to by all those using church computers?		
2. Is a file backup copy being secured on church property and another backup copy taken, at least on a weekly basis, to an off-site location?		
3. Is there a backup on each original software product (purchased or in-house developed)? Are the backup CDs being secured on church property?		
4. Are backup procedures performed before new software upgrades are installed?		
5. Are external labels or markings accurately prepared and placed on the backup device?		
6. Are working papers/data input papers kept until the next backup has been completed?		
7. Does the church have a backup off-site facility established (contingency plan) in case of a computer disaster (i.e. fire, flood, etc.)?		
8. Are daily backup procedures monitored to ensure they are strictly followed?		
9. Has the CD been tested to be sure the backup procedures are working?		
Additional Questions/Explanations:		
L. Local Area Networks (LAN)		
1. Is one person responsible for administering the LAN operations?		