APPENDIX B

PASSWORD PROTECTION

The payroll system provides password protection as a standard feature. If you do not wish to implement a password, you may change one or both passwords to blanks. This will allow you to access the system by simply hitting ENTER when prompted for a password.

It is important to note that password protection only prevents the payroll programs from being used. The password does not prevent copying of the payroll system's data files, and does not prevent an unscrupulous person from erasing or otherwise damaging your data files. In order to protect the files themselves, protection must be provided at the operating system level. At this writing, IBM PC-DOS does not have any facilities for protecting files, but some "shell" programs (commonly found in use in conjunction with Local Area Networks) have operating system level passwords.

The best security for your data files is to keep them on floppy diskettes in locked storage. If you use password protection, keep in mind that it only protects against the use of the payroll system by persons who are not experts in programming.

All Datasmith payrolls are shipped with unprotected source code included. While it is important to our customer support procedures that you have it available for emergencies, access to the source code and the file layouts in this manual must be denied to all users who are not to have unrestricted access to the system. If someone has access to the source code and some knowledge of BASIC, he can determine how the password protection scheme works by simply examining the code or printing the contents of certain critical program variables.

By using only the compiled programs we send you, and locking the source code (all of the .BAS files) in a safe place, you can provide yourself a greater level of security, since these programs have been translated to machine language by the compiler. While it is theoretically possible to determine how password protection works by examining the machine language code, it is an extremely difficult and time-consuming process.

To assure maximum protection against unauthorized users, be sure to remove the Technical Notes section, including all File Layouts, from this manual and lock it in a safe place. While the passwords are stored in an encrypted form, access to these documents would greatly simplify their decryption by an unfriendly or mischievous person.

USING PASSWORD SECURITY

Two levels of password protection are provided. The highest level, called the "Security Officer" or "Master" allows access to all the payroll functions. The Security Officer may also change both passwords at will. The second level of protection, called the "User", has access to all but certain critical functions. The following functions are denied access to someone using the "User" Password:

> 1.   *Display or change of the Security Officer password.*
> 2.   *Year End Initialization..*
> 3.   *Change of an employee number.*
> 4.   *Change of a payroll perod ending date.*
> 5.   *Un-Initialization of a prior period payroll.*

When password protection is implemented, the system reads the passwords stored in the master file when the program is first started and prompts for a password. The video display is inhibited during password entry so the password entered does not appear on the screen. This prevents an unauthorized person from being able to see the password when it is entered.

Three tries are given to enter the correct password. If the correct password is not entered, the program terminates and control is returned to the operating system.

> NOTE: *The sample data provided with the system uses **PW1** as the security officer, and **PW2** as the user. You should not normally use these widely-known passwords for your own master files.*

If you are using the system to run several payrolls, each master file <u>may</u> have a different password. Changing the data path will result in the system asking for the password appropriate to the new path, unless the payroll in the new path uses the same password entered by the operator for the current payroll. This allows the user to create "universal" and "local" passwords for multiple-payroll operations.

If there is no master file found using the path specified, the system will not prompt for a password, but will allow the creation of a new master file. In this case, the passwords are specified by the operator as part of the "Set Company Data" function.