

White Paper

FootPrint Software for Obtaining Compliance
with
CFR Part 11, Electronic Records and Electronic Signatures

FootPrint Software:

Is designed to provide electronic records and signature security to programs using Windows Operating Systems running on both standalone 95/98 and NT computer platforms. (see attachment I for Part 11 requirements and FootPrint functionality)

Description of Compliance Environment:

As of August 1997, Part 11 regulations have been mandated. These regulations "set forth the criteria under which the FDA considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper."

There is **NO** grandfather clause.

Example **FDA 483**:

"...In addition, we further request details regarding steps your firm is taking to bring your electronic cGMP records into conformance with the requirements of 21 CFR Part 11; Electronic Records; Electronic Signatures. ...This inspection disclosed deficient controls in the laboratory electronic record keeping system, which is used for maintaining chromatography and audit trails. In addition to a response to the deficiencies noted earlier in this letter, please outline your firm's global corrective action plan, including timeframes for correction, to address this Part 11 issue..."

Current Part 11 Solution Platforms:

Documentum
Nu-Genesis
SQL*LIMS
Wonderware

Software programs listed above are based on client-server platforms, and address audit trail requirements via file snapshots taken and stored at prescribed time intervals. Various methods are used to parse data for changes.

Description of FootPrint (FP):

1. At its core, FP is a sophisticated variation of a keystroke logger. This implies that when FP is active, any keystroke made during the session will be recorded in the Part 11 audit trail. Unique to FP is the audit trail or history format, that not only stores raw data changes but also interprets keystrokes into human readable format. (see attachment II)
2. FP can be customized and trained to look for unique commands such as <delete>, <close> or other application specific commands that modify or store a file. (see attachment III)
3. FP can be trained to monitor different applications, including MS Word, Excel, and Access applications (see attachment IV). Custom instrument software running in a registered file format can also be monitored.
4. FP history (audit trail) and setup can be secured based on password/system management hierachy. (see attachment V)
5. Installation is menu driven. Operation is straightforward. Training will be provided via phone support and documented help files.

Current Status of FootPrint

FP is ready for beta-testing on the 95/98 Windows platform. Plans are for a 2 month use/feedback interval. After which FP will be modified, where possible, to meet generic and unique customer requirements. Integration of Windows NT/2000 capability will be ongoing. Installation will be via internet download where capable, CD media will be used as optional installation vector.

FP is being developed in accordance with the System Life Cycle approach to software development. Source code is available for escrow and auditing under confidentiality agreement.

Stable platform, market ready by Sept 01, 2001.

Projected Cost Structure

\$500 (five hundred dollars) multiple use application per computer.

\$200 (two hundred dollars) single use application per computer.

Installation, training, one year phone support.

Custom programming will be contracted at negotiated rates.

Volume discounts are available.

Attachment I

ASSESSMENT OF FootPrint FUNCTIONALITY VS. PART 11 REQUIREMENTS

SUBPART B – ELECTRONIC RECORDS

(Key to Compliance Codes: Y = Yes, C = Customer Responsibility, V = OEM Vendor)

11.10 Controls for Closed Systems

Section	Issue	Compliance	Status
11.10	Validation of user systems	C	Validation is a customer responsibility.
11.10 a	Are invalid or altered records discernable?	Y	Altered records can be discerned through the audit trail.
11.10 b	Capable of generating accurate and complete copies of records in human readable and electronic form	Y	Records stored in secure database.
11.10 c	Protection of Records to allow retrieval throughout their retention period	C	Backup and Archive tools provided in XXX software. Dependent upon customer's operating system and/or 3 rd party data management software.
11.10 d	Limiting system access to authorized individuals	Y	Through user name and password, as defined in section 11.200 a 1.
11.10 e	Use secure, computer-generated, time stamped audit trail that independently records the date, time of operator entries/actions that create, modify, or delete electronic records.	Y	Part of audit trail.
11.10 e	Record changes shall not obscure previously recorded information.	Y	Copy of file before changes are made is archived.
11.10 f	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	C,V	Dependent on application.

Section	Issue	Compliance	Status
11.10 g	Assure that only authorized individuals can use the system, e-sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	C	XXX is restricted to those with electronic signature access. Customer SOPs required for full compliance.
11.10 h	Use of device (e.g. terminal) checks to determine the validity of the source of data input or operational instruction.	C,V	Dependent on application, customer SOP's.
11.10 i	Personnel who develop, maintain, or use e-record/signature systems have the education training, and experience to perform assigned tasks.	C	Records and Customer SOPs required for full compliance.
11.10j	Establish written procedures for accountability and responsibility of activities under their e-signatures.	C	Customer SOPs required for compliance.
11.10 k.1	Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	C	Customer SOPs required for compliance.
11.10 k.2	Revision and change control procedures with audit trail to document time-sequenced system documentation changes.	C	Customer Change Control SOPs required for compliance.

11.50 Signature Manifestations

Section	Issue	Compliance	Status
11.50 a	Signed e-records shall contain information that includes; <ul style="list-style-type: none"> The printed name of the signer The date and time of signing The meaning of the signing (review, approval, responsibility, or authorship). 	C	Customer SOPs required for compliance.
11.50 b	Items in 11.50 a are included as part of human readable form of electronic record, such as display or printout.	C	As in Remarks of 11.50 a

11.70 Signature/record Linking

Section	Issue	Compliance	Status
	Signatures are linked to their respective e-records to ensure they cannot be excised, copied, or otherwise transferred to falsify an e-record by ordinary means.	Y	Electronic records with e-signature linkage are secured in database audit trail.

SUBPART C – ELECTRONIC SIGNATURES

11.100 General Requirements

Section	Issue	Compliance	Status
11.100 a	Each electronic signature is unique to the individual and not to be reused, or reassigned to anyone else	C,V	XXX usually do not allow concurrent duplication of e-signatures. Assignment and use of e-signatures is per customer SOPs.
11.100 b	Identity of the individual is to be verified before sanctioning an e-signature.	C	Customer SOPs required for compliance.
11.100 c, c.1, c.2	Electronic signatures general	C	Customer compliance issues requiring notification to the FDA, not related to XXX functionality. Customer SOP's needed.

11.200 Electronic Signature Components and Controls

Section	Issue	Compliance	Status
11.200 a	Electronic signatures that are not based upon biometric signatures shall:		
a.1	Employ at least two distinct identification components	Y	User name and password in XXX Security
a.1.i	When a series of signings are made during a single continuous period of controlled access, the first signing shall be executed using both signature components, and...	Y	Initial log-in in XXX Security
	Subsequent signings shall be executed by at least one component of that individual's e-signature.	Y	Userid, in conjunction with audit trail.
a.1.ii	When an individual executes one or more signings not done in a single continuous session, both components shall be executed at each signing.	Y	Re-log-in, as in 11.200 a.1.i .
11.200 a.2	Be used only by their genuine owners	C,V	Depends on XXX Vendor Security that should not allow contemporaneous use of the same combination of User ID and passwords. Customer SOPs also required for compliance.
11.200 a.3	Be administered such that use of a signature by a non-owner (counterfeit) requires the collaboration of two or more individuals.	C	Customer SOPs required for compliance.
11.200 b	Biometric signatures shall be designed to be used only by their genuine owners.	C	Customer SOPs required for compliance.

11.300 Controls for Identification Codes/Passwords

Section	Issue	Compliance	Status
11.300	Controls for e-signatures based on ID codes in combination with passwords must:		
11.300 a	Maintain uniqueness, i.e. such that no two individuals have the same combination.	Y	As in 11.200 a 3
11.300 b	Ensure that ID codes and passwords are periodically checked, recalled, or revised.	C	Currently this is the System Manager's responsibility. Addressed with Customer's SOPs.
11.300 c	Disable an ID code or password that is lost or otherwise compromised	Y,C	User ID and passwords may be removed in XXX. Customer SOPs required for compliance.
11.300 d	Detect and report attempts at unauthorized use to the system security and/or management.	Y,C	Audit trail tracks any entry into database. Customer SOPs required for compliance.
11.300 e	Provide functional testing of devices that generate password or id information.	C,V	Customer SOPs required for compliance.

Attachment II

During a FootPrint session an Excel file “FP Example” was opened and monitored. Attachment II is the audit trail for this session.

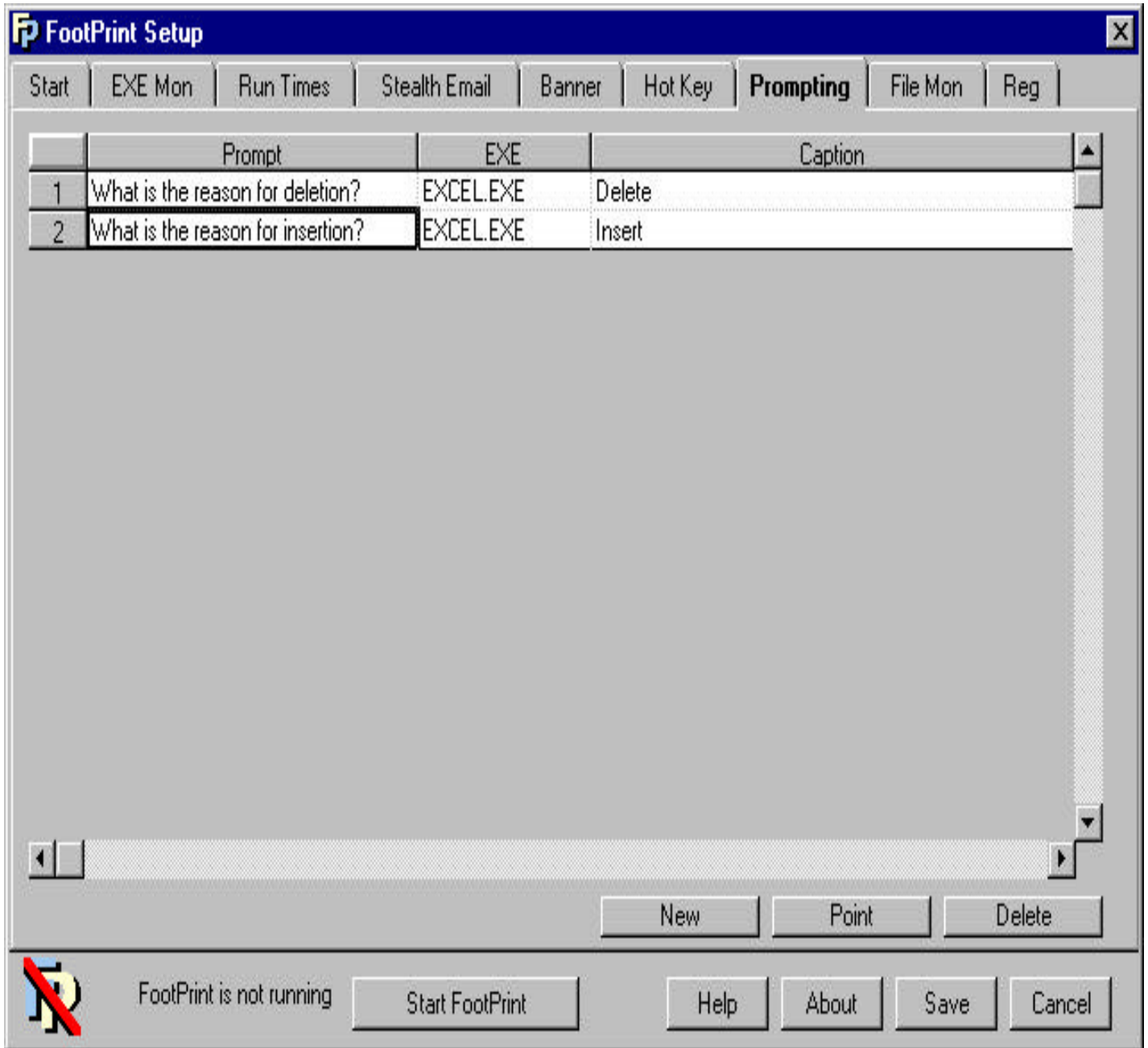
1. When a file is opened, FootPrint automatically makes a time stamped copy of the file before changes are made.
2. A cell was changed by using the <delete> key, as demonstrated in “raw” column, row 1.
3. The new value “4.43526” was input and recorded in both “formatted” and “raw” data columns, row 2.
4. Upon exit from the spreadsheet, the user is prompted for an explanation for the change, which is captured in the “explanation” column , row 4.
5. Full user name and unique ID were input and subsequently recorded in the “explanation” column, row 4. Changed file is saved.
6. Since a change was made , the saved file in step 1 is stored to the secure database. This allows for both before and after change , file comparison..

All records are stored in a single, password protected file “fp.mdb” as shown in the bottom screen tray. Reports can be customized. Captured fields are user defined with several other “subject fields” available, such as “elapsed time”, which would display time spent during the session.

	Workstation	User	Date	Start	Exe	Caption	Formatted	Raw	Explanation
1	RICHMOE	richmoe	12/5/00	10:44:28 AM	C:\PROGRAM FILES\MICROSOFT OFFICE\OFFICE\EXCEL.EXE	Microsoft Excel - FP EXAMPLE		<DELETE>	
2	RICHMOE	richmoe	12/5/00	10:44:32 AM	C:\PROGRAM FILES\MICROSOFT OFFICE\OFFICE\EXCEL.EXE	Microsoft Excel - FP EXAMPLE	4.43526	4.43526	
3	RICHMOE	richmoe	12/5/00	10:44:39 AM	C:\PROGRAM FILES\MICROSOFT OFFICE\OFFICE\EXCEL.EXE	FP EXAMPLE			
4	RICHMOE	richmoe	12/5/00	10:44:46 AM	C:\PROGRAM FILES\FOOTPRINT\FP.EXE	FP EXAMPLE.xls	transcription errors. john doe 123-45-6789	transcription errors. john doe 123-45-6789	C:\My Documents\FP EXAMPLE.xls has been changed. Please explain. : transcription errors. john doe 123-45-6789
5	RICHMOE	richmoe	12/5/00	10:45:05 AM	C:\PROGRAM FILES\MICROSOFT OFFICE\OFFICE\EXCEL.EXE	Microsoft Excel			

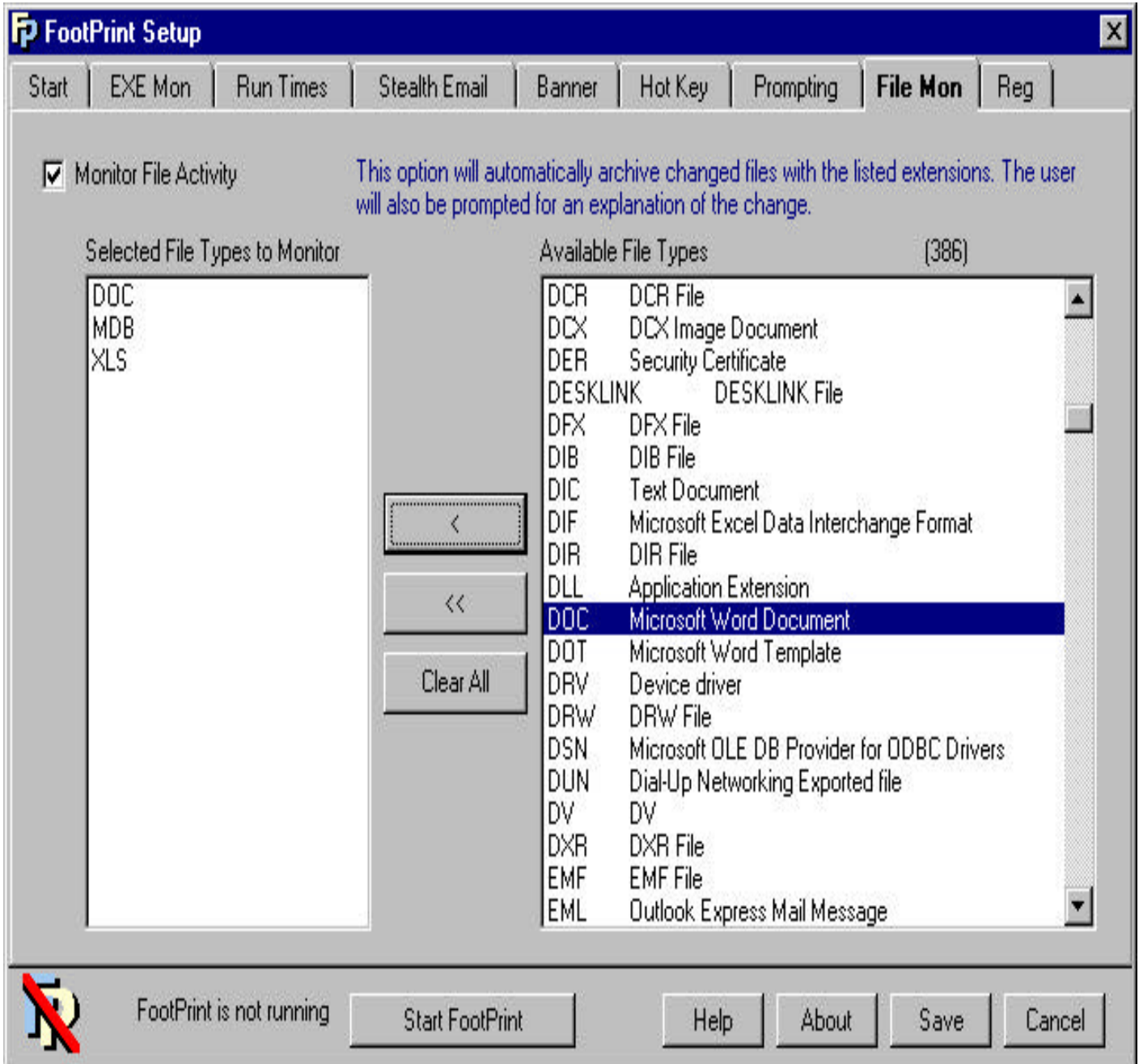
Attachment III

During the setup phase of FootPrint , softkey commands can be captured. For example, both the “delete” and “insert” command will be monitored with the setup displayed below. During a live Excel session, any use of these commands will be followed by the question shown in the “prompt” column, rows 1 and 2. The subsequent user input becomes part of the permanent audit trail.



Attachment IV

During the setup phase of FootPrint, any executable that uses registered file names can be monitored. In the example below, Word, Access, and Excel files have been chosen from the list of file types on the right.



Attachment V

Both FootPrint History (audit trail) and Setup can be secured by password. Demonstrated in the “Password” box below. This allows for program function and security control at the system manager level.

