Terminal User Security Guidelines

1. Fulfillment of DP asset protection responsibilities is mandatory and may be considered a condition of employment.
2. DP assets may be used *only* for IBM management approved business.
3. Your password is IBM confidential – treat it accordingly.
4. Passwords must be at least 4 alphanumeric, 5 alphabetic, or 6 numeric characters in length, not trivial and changed at least every 60 days.
5. Do not share your password.
6. All classified data – including system work spaces – must be protected accordingly.
7. All IBM Confidential-Restricted data must be encrypted for transmission to or from remote terminals unless hard wired to the host.
8. Do not enter or access Registered IBM Confidential data without consulting with the Recorder of Registered Documents and the computing service administrator.
9. All types of output must have its classification properly labeled.
10. Confidential data sets and work spaces should be access controlled to prevent unauthorized use.
11. Terminal must not be left unattended when logged-on.
12. Log-off after each session.
13. Dial-up numbers are not to be posted.
14. *Tektronix* users erase screen before turning power off.
15. Confidential waste and residual data must be disposed of properly.
16. Be familiar with Endicott Operating Procedure 500-07.
17. Report any suspected violations or misuse to management.

8/16/82

IBM

Endicott Product Security
X7420