

Treasury Documentation**Subject:** Password Rules, Data Collection Distribution System (DCDS)**For:** EMPLOYEE HANDBOOK
SECURITY GUIDE**Also See:** ET-03175, 80

Identification	BT-03075 Bulletin
Effective Date	5-1-2012
Replaces	BT-03075 (1-1-2010)
	Page 1 of 1

Each employee with access to the Data Collection Distribution System (DCDS) system must:

- Create and use a strong password within the DCDS environment; i.e., each password must contain a combination of alphabetic characters and numeric characters. Each DCDS password must contain:
 - Eight to a maximum of 30 alphanumeric characters.
 - Two numeric characters, neither of which may be the first character of the password.
 - Four distinct characters – no more than three alphabetic characters in a row.
- Never include the user ID as part of the password.
- Avoid using dictionary words or acronyms as passwords and choose passwords that are not easy to decipher and not trivial, predictable, or obvious.
 - Trivial passwords include common words like “secret,” “password,” “computer,” etc.
 - Predictable passwords include days of the week, months, only one or two characters different than the previous password, or a keyboard pattern such as “qwertyui.”
 - Obvious passwords include names of persons, relatives, pets, cities, streets, UserID or user name, an anagram of UserID, Social Security number, birth date, nickname, car license plate, etc.
- Change the DCDS password at least every 45 days.
- Keep the DCDS password confidential; i.e., do not share or divulge a password to anyone.
- NOT write down the DCDS password.
- Never reuse a password when required to change it.

If an employee suspects the DCDS password is known by anyone or its security is in doubt, **change the password immediately and follow the notification requirements of Policy ET-03180 Incident Reporting.**

The DCDS account will be locked after five unsuccessful attempts to log in. Contact the Office of Human Resources for issuance of a new password.

End