

Drake University Password Policy

Effective February 29, 2009

The **purpose** of this policy is to protect Drake and personal files from intrusion, deletion, and alteration by unauthorized parties, and to prevent the use of Drake systems by unauthorized parties. A password policy is one element is the overall Drake computer security plan.

The **password policy states** that that all possessors of a Drake email account must should protect it with “strong” password as explained below, and should change that password at least once a year.

What is a Secure Password?

Every strong password must contain at least eight characters, including one from each of the four categories below:

- i. An uppercase letter
- ii. A lower case letter
- iii. A number
- iv. One of the following characters: _!@#\$.

Within these restrictions, passwords should be easy to remember, because they should not be written down. Examples are “I_loveCubs2009” to “Philosophy#1”. Users should create passwords which they can remember easily.

Changing Passwords

- i. A password may be used for one year but must be changed at least once within the next 365 days.
- ii. Each user will receive warnings in advance of the date that their password must be changed. These warnings will be by Drake email 30 days, 14 days, 7 days, 3 days and 1 day before the expiry date.
- iii. At the end of the warning period, access to an account with an unchanged password will be locked.
- iv. If a user is locked out because the password has expired or has been forgotten, the Drake Service Center (Help Desk) 271-3001 or departmental technical staff will create a temporary secure password. Users will wish to change that to a private password immediately, using the Drake Password Gateway in BlueView.
- v. A password which has been used once cannot be reused.
- vi. If a user enters a password incorrectly three times in a row, the account cannot be used by anyone for ten minutes.