Policy #: IT.008–Password Controls

Governed by: IT Administration
Approval Date: November 1, 2016 **Last Updated:** November 1, 2016
Purpose: CEO Password Controls

CEO User Network Passwords and Controls

Password control and password policy are of high importance. Passwords allow/deny access to network resources. This can include access to files/folders/PCs/Laptops/Printers etc. The password policy for access to the network must meet the following requirement (which applies to all user accounts):

- Password must meet complexity requirements (must contain at least one each of Alpha, Numeric and Character)
- Minimum characters: 7
- Maximum age of passwords: 60 Days
- Cannot reuse 3 of the previous passwords
- If password is entered incorrectly 3 times the user is locked out for a minimum of: 15 minutes
- If password is entered incorrectly 5 times the account will lock automatically disable for security purposes to ensure that there is no guessing of passwords from an unauthorized individual
- User accounts can only be unlocked by contacting IT.

There is absolutely no need to share password details with anyone other than with a member of the IT Department; this is to ensure that they can support you operationally. Any passwords passed to IT will be kept under the strictest confidence. IT reserve the right to requests any user's password at any stage to ensure network compatibility, integrity and security and operational needs, even if a user is using a personal password. Users are entitled to change their passwords at any time by pressing CTRL+ALT+DLT on their keyboard and select "Change Password" and as long as the password policy requirements are met.

For further assistance please refer to the Password Guidance document on the Intranet.