Delaware State University

University Area(s) Responsible: Office of Information Technology
Procedure Number & Name: 8-06 Password Policy
Approval Date: _____

I. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of required password change for users of Delaware State University ("University") computer systems. Passwords are an important aspect of computer security; poor password policy may result in unauthorized access and or exploitation of University resources. By following the policy and procedures users will help in reducing this risk and gain the ability to unlock and or change their passwords through self-service. A robust password policy will also reduce the number of calls to the Central Help Desk (CHD) for password resets.

II. Scope

This policy and included procedures apply to all users of University computer systems.

III. Policy

Initially users whose password age is nearing the maximum time limit will begin receiving email notifications along with detailed instructions. These notifications will alert the user that they will be required to establish challenge questions and reset their Active Directory password within 21 days of password expiration. The user will continue to receive messages daily until they establish their challenge questions and perform the required password change. Students will be required to change their passwords every 180 days and faculty/Staff every 90 days. Should a student or faculty/staff member fail to establish their challenge questions and perform a password change prior to the end of the 21 days they will cease receiving notifications and may* need to contact the helpdesk for assistance.

*Active Directory password can be changed by students by logging into at any lab computer, faculty/staff can change passwords on any computer attached to the administrative network.

IV. Password Rules

Faculty/Staff	
Enforce Password History	Last 6 passwords remembered
Maximum password age	90 days
Minimum password age	0 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Account lockout duration	30 minutes
Account lockout threshold	6 invalid logon attempts
Rest account lockout counter after	30 minutes

Students	
Enforce Password History	Last 4 passwords remembered
Maximum password age	180 days
Minimum password age	0 days
Minimum password length	8 characters
Password must meet complexity requirements	Enabled
Account lockout threshold	0

V. Self-service Password Change/Reset Procedures

Faculty/Staff

Active Directory/Windows Login

- Ctrl-Alt-Delete at any administrative computer
- 21 day Password expiration notification via email with web instructions
- Challenge question via main campus and my.desu.edu web pages "Directory" Link: https://directorysearch.desu.edu/DirectoryUpdate/
- Contact Local Helpdesk
- Contact Central Helpdesk

Banner

- PIN reset via instruction on each page where PIN is required
- Banner password reset via call to CHD or local Helpdesk assistance via through banner web/Putty applications
- Contact Local Helpdesk
- Contact Central Helpdesk

Telecomm

- Voicemail password reset via call to CHD or local Helpdesk assistance

Students

Active Directory/Windows Login

- Ctrl-Alt-Delete at any lab computer
- 21 day Password expiration notification via email with web instructions
- Challenge question via main campus and my.desu.edu web pages "Directory" Link: https://directorysearch.desu.edu/DirectoryUpdate/
- VIA ODELT (Distance education) office as required for Blackboard support
- Local Helpdesk
- Central Helpdesk

Banner

- PIN reset via instruction provided on each page where PIN is required
- Contact Local Helpdesk
- Contact Central Helpdesk