I. Purpose of Policy/Policy Statement
   A. In order to comply with industry standards and to increase the security of our IT systems, the password policy contained herein would require better password complexity, as well as periodic password changes. This would be implemented in conjunction with our Identity Management System, which will synchronize the password to multiple resources.

II. Detailed Policy Statement
   A. Hamline passwords would be required to be at least 8 characters long, with at least 1 uppercase character, 1 lowercase character, and 1 numeric character. Only numbers and letters would be allowed, as some applications don’t allow special characters in passwords.
   B. Passwords would need to be changed every 180 days. When changing their passwords, users would be unable to re-use the two most recently used passwords.
   C. A corresponding lockout strategy will be implemented. Five incorrect login attempts in 30 minutes would cause an account to be locked for 30 minutes, but the lockout could be cleared by the user performing a self-service password reset.
   D. A corresponding auto-logoff mechanism would terminate a logged-in session after a predetermined time of inactivity.

III. Applicability
   A. Policy applies to all Hamline computer accounts, including staff, faculty, student, and shared/departmental accounts.

IV. Definitions
   A. Definitions of terms in policy and applicable procedures.

V. Cognizant Offices/Getting Help
   A. Primary support would be the helpdesk – itsupport@hamline.edu x2220

V. Policy Authority
   A. ITS – CIO.
VII. Related Policies/References for More Information
   A.

VIII. Implementation Procedures
   A. Policy would be enforced by the Identity Management System, as well as Active Directory. Users could set up challenge/response questions to help themselves with password resets for forgotten passwords.