Northeastern University

INFORMATION TECHNOLOGY SERVICES

Effective Date: July 1, 2012

Date Revised: August 20, 2014

Supersedes: N/A

Related Policies: University Password Standards

Responsible Office/Department: Office of Information Security

Keywords: Password, System access

Policy on Enterprise Passwords

I. Purpose and Scope

Passwords to the University Enterprise Systems are vital part of securing access to University Data; therefore the University mandates that all accounts be secured using a password of a significant minimum complexity.

II. Definitions

Enterprise System: Any system which is part of the Single Sign-on Authentication, or serves as part of the University core system.

NU User Accounts: Accounts on the system without elevated privileges.

Single Sign-On (SSO): Accounts which synchronize with the LDAP or Active Directory to pass authentication through several applications.

Third Party Vendor/Providers: An outside (non-NU) organization contractually engaged by the University to provide one or more services to students, faculty and or staff, whereby the affiliate may legitimately have the need to access institutional information

Vendor: An outside (non-NU) organization contractually engaged by the University to provide one or more services to students, faculty and or staff, whereby the affiliate may legitimately have the need to access institutional information.

System Accounts: Highly privileged accounts.

Information Assets: Data passed on or through University information systems. Also includes equipment through which data is passed, processed, analyzed, modified, stored and/or destroyed.

Institutional Information:

- Information used in planning, managing, directing, controlling, operating or auditing a function of the University.
- Information referenced or required for use by one or more functions, departments and/or units within the University, including students and affiliates.

- Information represented in an official University document, report or submission.

- Information that may be created, developed or enhanced by the University, or by which the University derives value from possession and/or use.

Sensitive Institutional Information: Institutional information considered to be administratively or legally privileged due to value, content, regulation, and/or consequences of unauthorized or inappropriate access or use. Restrictions may be imposed by reason of business rule, legal, ethical or other legitimate constraint.

Information that personally identifies an individual. This classification may not apply when the information is aggregated, or when sufficient identifying information is removed so as to make personal identification impossible.

III. Policy

Whereas institutional information is one of the most valued assets of the University, and whereby access carries with it the responsibility to safeguard and protect institutional information from loss of confidentiality, integrity and availability, it is the policy of the University that:

Part 1 - Password Requirements for Northeastern University Accounts

Passwords to all Northeastern University Enterprise accounts, third-party system accounts or any system which contains or accesses University Information Assets, must meet the defined University Password Standards.

Part 2 - Password Requirements for Third-Party Providers

1. Access to University data when provided through a third-party application should have established access controls using credentials and password synchronized through the University's LDAP or AD systems, to ensure an appropriate strength of password complexity and adherence to the University Password Standards.
2. Where access to third-party applications cannot be established through the use of LDAP or AD systems, the vendor will establish password controls which meet the University password complexity standards, except where technically infeasible.
3. Appropriate controls will be implemented as are technically, operationally and financially feasible to ensure data is safeguarded consistent with University policy, law and regulation.

Section 3: Password Requirements for Noncompliant Systems

For systems not technologically able to reach the minimum password requirements as stated in **Section 1** and **Section 2**, passwords must be at least 10 characters in length, if possible; and systems must incorporate industry standard security procedures to protect user accounts.

IV. Additional Information

Any system which houses protected information as defined by the Data Protection Policy must have appropriate password controls. Any third-party system which cannot meet technical requirements must have appropriate policy controls applied and have had the methodology approved by the Office of Information Security.

V. Contact Information

Office of Information Security – OIS@northeastern.edu