Policy 5.15
Enterprise Password Policy

Responsible Official: Enterprise CIO and Sr. Vice Provost for Library Services and Digital Scholarship
Administering Division/Department: LITS: Library & IT Services
Effective Date: May 01, 2014
Last Revision: July 20, 2017

Policy Sections:

Overview

Passwords are used in conjunction with individual network ids (netids) to provide authenticated access to Emory IT resources. As such, it is important that the passwords used to protect access to Emory IT resources are of sufficient quality that they cannot easily be guessed or cracked. This policy establishes password requirements in furtherance of this objective.

Applicability

This policy applies to all Emory information systems where passwords are utilized and to all users of such systems. Systems implemented after the effective date of this policy that do not rely on enterprise authentication systems or enterprise password management solutions must comply immediately.

Policy Details

Passwords for Emory IT resources shall comply with the following requirements:

User Requirements

- Users are required to choose strong passwords that meet the password composition requirements indicated below and are not otherwise easily guessable.
- Users must change their passwords in accordance with the Password Change Requirements noted below and must not reuse previously used passwords
- Users must NEVER share their authentication credentials (e.g. passwords, PINs, tokens) or log in for others. Likewise, users must NEVER use the authentication credentials of anyone else.
- Users must not use the same password for accessing Emory IT resources as they use for non-Emory applications and systems. Users should, however, still choose strong passwords whenever utilizing non-Emory applications and systems for Emory related purposes.
- Users must not write down or otherwise store their password in an unprotected manner (e.g. unencrypted).
- If a user knows or suspects that their password has been shared or compromised, it must be changed immediately (for every account that uses the same password).

Password Composition Requirements

- Minimum Password Length: 9 Characters
- Maximum Password Length: 30 Characters
- Password Complexity: Passwords must contain at least 2 alphabetic characters (A-Z, a-z), at least 2 non-alphabetic characters (spaces, numerals, punctuation and/or special characters appearing on a standard U.S. PC keyboard).
- Password Constraints: The userid/netid cannot be part of the password, and the password cannot contain more than 2 consecutive characters that are identical.

Password Change Requirements

- Maximum Change Interval: 365 Days (90 days for system/network administrators and individuals with access to cardholder data or cardholder data systems)
- Minimum User-Initiated Change Interval: 1 Day
- Password Rotation History: 24 Passwords

Account/Password Lockout Requirements

- Lockout Threshold: 10 Unsuccessful login attempts
- Lockout Duration: 30 Minutes

IT System Requirements

- Emory IT resources shall enforce the Password Composition, Password Change, and Account/Password Lockout Requirements documented above via technical means whenever possible.
- IT resources shall automatically reject any password selection that matches passwords currently held within the password rotation history for the account
- Keyed passwords must never echo or display in any readable form on the screen of the log in device.
- IT Resources must never store passwords unencrypted
- All Emory application systems must display a warning notice at each interactive login when technically feasible. The text of warning banner shall read as follows:

> "You are about to access a computer system maintained or made available by Emory University and/or Emory Healthcare that is intended for authorized users only. Unauthorized use of this system is strictly prohibited and may be subject to criminal prosecution. By proceeding, your use of this system constitutes your acceptance of Emory's IT Conditions of Use and other applicable policies and your consent to monitoring, retrieval, and disclosure of any information within this system for any purpose deemed appropriate by Emory University or Emory Healthcare, including law enforcement purposes and enforcement of rules concerning unacceptable uses of this system."

When technically feasible the application system should provide users with the ability to follow a hyperlink within the warning banner to view Emory's IT Conditions of Use Policy.

Exception to IT System Requirements

If, after undertaking a good-faith investigation of current state of the art technical alternatives, the business owner of an IT resource determines that it would be unduly burdensome to implement the Password Composition, Password Change, or Account/Password Lockout Requirements, the business owner of an IT resource shall request an exception to this policy, using forms to be prescribed and maintained by the LITS:Enterprise Security Team. Factors to be considered in reviewing such requests shall include, but shall not be limited to:

- The type of system involved
- Its connection to other Emory IT infrastructure and networks
- Less burdensome alternative security measures that are capable of implementation

Exceptions may be granted at the sole discretion of Emory's Chief Information Security Officer (CISO) after reviewing the business owner's request. Exceptions are limited to one year in duration, and may be revoked upon the CISO's determination that the system operating under the exception is a security risk to the enterprise.

Password Reset Requirements

- Every request to reset a password or unlock an account must be met with a challenge/response validation process

that is sufficient to confirm the requestor's identity and that the requestor is authorized to access the account.

Sanctions:

- Failure to comply with this policy may have legal consequences and may result in:
  - Suspension or termination of access;
  - Disciplinary actions (up to and including termination of employment) in accordance with applicable university policy.

Related Links

- Current Version of This Policy: http://policies.emory.edu/5.15

Contact Information

Subject	Contact	Phone	Email
Clarification of Policy	LITS Security Team	via listserv	securityteam-l@listserv.emory.edu

Revision History

- Version Published on: Mar 13, 2016 *(Updated Sanctions Language)*
- Version Published on: Mar 13, 2016 *(Updated department names and titles)*
- Version Published on: Aug 29, 2014 *(Initial Publication)*