End User Password Minimums

Standard ID
IOT-CS-SEC-117

Published Date
9/27/2006

Effective Date
4/1/2007

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
06.0 Access Control (PR.AC)
  06.1 PR.AC-1
  06.1.1 Account Management

Purpose
The State of Indiana advises all capable systems to require complex passwords for access. This step strengthens the State’s password protection scheme which remains the primary method of secure access to information systems. The requirements set forth in this Standard refer to Active Directory passwords.

Scope
IOT Supported Entities

Statement
Below are the requirements as it relates to end user passwords:

- Minimum password length: 8 characters
- Password complexity: Systems shall enforce complex passwords ensuring that passwords are made up of at least three of the following attributes: upper and lower case letters, numeric characters, embedded spaces or special characters. Active Directory setting = enabled.
- Password history: 24 previous passwords unavailable for reuse
- Minimum password age: 1 day
- Maximum password age: 90 days
- Account lockout duration: 30 minutes
- Account lockout threshold: 15 attempts
- Reset lockout account after: 15 minutes

Agencies may require more stringent requirements due to regulatory requirements. In which case, agencies shall work with IOT to make appropriate setting changes, no less stringent that the requirements within this Standard.

Roles
All Personnel
IOT Personnel
Responsibilities
All personnel shall abide by the password requirements written within this Standard and shall not post or share passwords with others. Agencies shall adopt complex passwords for all compatible systems, document any exceptions to complex password requirements and communicate and educate staff on proper use of passwords. IOT shall provide support for use of complex passwords.

Management Commitment
Management is responsible for ensuring their agency is meeting the requirements written within this Standard.

Coordination Among Organizational Entities
Agencies shall coordinate with IOT where necessary to meet additional regulatory requirements related to this Standard.

Compliance
Monthly Active Directory reports.

Exceptions
No exceptions.