PCI compliance password requirements

rdavis@foregenix.com - 2018-01-11 - Comments (0) - PCI Compliance

As mandated by the Payment Card Industry Data Security Standards (PCI DSS) are clearly stated within Requirement 8 of Version 3.0 of the PCI DSS standards. Specifically, the PCI compliance password requirements are the following:

- Require a minimum length of at least seven characters.
- Contain both numeric and alphabetic characters.
- Users to change passwords at least every 90 days.
- Password parameters are set to require that new passwords cannot be the same as the four previously used passwords.
- First-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use
- User accounts are temporarily locked-out after not more than six invalid access attempts.
- Once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.
- System/session idle time out features have been set to 15 minutes or less.
- Passwords are protected with strong cryptography during transmission and storage.

Tags

Compliance

Passwords

PCI

requirements