

Case Study: Penn State and Password Practices

Penn State participated in the eAuthentication/Higher Ed pilot in 2005, which included a credential assessment by GSA. As a first step, we are putting the processes and policies in place to be compliant as NIST LOA 1 and used a combination of feedback from this credential assessment, the Entropy Tool, and NIST guidelines to determine what was needed to reach this.

For LoA 1, PSU has a password policy for all passwords that include the following:

1. It must be at least eight characters in length (Longer is generally better.)
2. It must contain at least one alphabetic and one numeric character.
3. It must be significantly different from previous passwords in the case of changes.
4. It cannot be the same as the userid.
5. It cannot start or end with the initials of the person issued the userid.
6. It cannot include the first, middle, or last name of the person issued the userid.
7. It cannot contain three or more occurrences of the same character.
8. It cannot contain any special characters (blanks, single quotes, double quotes and so on).
9. It should not be information easily obtainable about you. This includes license plate, social security, telephone numbers, or street address.

We are also in the process of determining the best approach and starting communications for enforcing annual password changes and are very close to meeting requirements for LOA2 as well.

This is a first step toward defining the various LOA's and policies. A large part of this change hinges on identifying and engaging the stakeholders, since adoption requires departments to think differently about how they provide access to services and understand the value of risk assessments for services and credential service providers.

For more information, refer to <http://its.psu.edu/policies/password.html>.