Password Security Policy
08/01/22 AMW

Network and data security at Juniata College is highly dependent on the security of users' passwords. At the user level, passwords protect computers, files, and email accounts. At the organizational level, passwords protect the integrity of important systems and services. Any time a password is compromised, an opportunity for an unauthorized user to invade these resources presents itself.

Each individual is assigned a set of unique credentials, with required multi-factor authentication. Authentication is required of users before they can access College resources. Access to protected data, information, and resources via the College's IT infrastructure is limited to those individuals who have a business reason to know such information.

Users are responsible for safeguarding passwords along with other authentication mechanisms (such as user names, PINs, etc.) and are accountable for negligent disclosure of passwords per the College's *Ethical and Responsible Use Policy*, online at http://help.juniata.edu/policies/EthicalUse.pdf.

Passwords used to protect Juniata resources must:
- meet history, complexity, and length requirements and must be **changed annually;**
- be changed immediately if compromised;
- be considered high risk data and not be shared with anyone;
- be encrypted if sent electronically via methods outlined in the *Data Protection Policy*; and
- should not be stored in browser caches or other "auto complete" types of features available in browsers and other software.

Account lock out is enabled after a specific number of unsuccessful attempts for a specific period of time.

We provide access to an account self-service portal for users to change and reset their passwords without assistance from the Information Technology Help Desk. For instructions on how to sign up for the account self-service portal and to change your password, please visit the technology support site at https://help.juniata.edu/view_article.php?article=231.