

Scope

This Supporting Policy applies to all Hobart and William Smith (“HWS” or the “Colleges”) community members and Users, as defined in the Colleges’ Responsible and Acceptable Use of Electronic Resources Policy (“Acceptable Use Policy”), that are issued credentials (i.e. username and password) to access the Colleges network, technology infrastructure, or Electronic Resources as defined in the Colleges’ Acceptable Use Policy. This Supporting Policy is intended to supplement the Acceptable Use Policy. Defined terms within this Supporting Policy have the same meaning as their definition in the Acceptable Use Policy.

Purpose and Need

This Supporting Policy requires the use of robust passwords that must be changed at predetermined intervals. Passwords are an essential aspect of the security of the Colleges’ Electronic Resources and they provide an important first line of protection for the Electronic Resources, Institutional Data, and intellectual property that resides at the Colleges. Having a strong password is one way that each User can contribute to the community’s overall security. Strong passwords help the Colleges prevent unauthorized or inappropriate access to various Electronic Resources like email accounts, online library resources, student information systems, financial records, file repositories, learning management systems, and administrative/transactional systems.

Specifications and Guidelines

All Users must maintain a password that meets the following minimum requirements:

- Must be a minimum of 8 characters
- At least one upper case alphabetic character (A-Z)
- At least one lower case alphabetic character (a-z)
- At least one number
- No blank spaces

Passwords will automatically expire after 365 days and must be changed. All Users will be notified well in advance of their password expiring so that they may reset them without interruption in access to the Colleges’ network. All community members can manage their password at <http://password.hws.edu>.

All Users are expected to adhere to the following guidelines regarding their password;

- Never write your password down or store it electronically
- Avoid using repetitive or sequential passwords
- Change your password when notified to do so. Each time you reset your password, it will remain active for 365 days.
- Avoid constructing a password with any full word from any dictionary or a name.

Non-compliance

Failure to comply with this Supporting Policy may result in actions as specified in the Acceptable Use Policy.

Exceptions

There are no exceptions to this Supporting Policy.

Additional Information

For any additional information, visit the IT Services Web at www.hws.edu/ITServices.