

# Password policy and requirements

## How to reset your password

Visit <https://password.covenantseminary.edu> and follow the on-screen instructions.

For a full procedure, visit [Reset your password - detailed instructions](#).

**i** A personal email address is required to reset your password. All students and employees should have a personal email on file with the institution. Please contact [IT Services](#) with any questions.

### On this page

- [How to reset your password](#)
- [Expiration](#)
- [Complexity](#)
- [General guidelines](#)
- [How to choose a more secure password](#)

## Expiration

- Student passwords do not expire.
- Employee passwords expire every six months.

Employees are notified via email of an upcoming password expiration. These notifications come 2 weeks prior, 1 week prior, and 2 days prior to the expiration date.

## Complexity

Currently, passwords are required to have the following complexity:

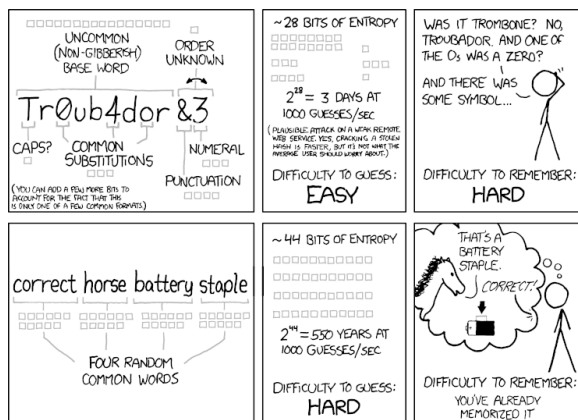
- Length of at least 8 characters.
- One uppercase letter
- One lowercase letter
- One number

## General guidelines

As employees of the institution, we are stewards of student information, which is governed by the Family Educational Rights and Privacy Act (FERPA). As such, we have a duty to our students to treat their information with the utmost care. Here are some general guidelines regarding your employee account.

- Never write down your password.
- Never share your password with anyone (including IT Services). If another person (employee or not) knows your Covenant Seminary employee account username and password, it is highly encouraged to change your password immediately.
- IT Services employees should not change your password for you. IT Services employees should assist you through the process of changing your own password.
- Consider using a password manager (e.g. Last Pass) to store your passwords in a secure and easily retrievable place (Contact IT Services for more information).

## How to choose a more secure password



THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.